حروب
تقنية المعلومات

كيف يشنها القراصنة والإرهابيون على البنية التحتية العالمية؟ وكيفية مواجهتها؟

فريج بن سعيد العويضي

حروب تقنية المعلومات

كيف يشنها القراصنة والإرهابيون على البنية التحتية العالمية؟ وكيفية مواجهتها؟

فريج بن سعيد العويضي

الرقم العالمي المتسلسل للكتاب ISBN: 978-9960-677-46-0

المحتويات

إهداء

إلى زوجتي الغالية وأولادي وأحفادي

نبذة عن المؤلف

المهندس فريج بن سعيد العويفي مستشار في مجال الاتصالات وتقنية المعلومات، تخرج من جامعة كنت في كنترباري المملكة المتحدة عام ١٩٧٣م. عمل نائباً لسفير خادم الحرمين الشريفين في المملكة المتحدة بمرتبة سفير في الفترة من ٢٠٠٣ - ٢٠٠٦ بدأ المهندس فريج العويفي خدمته ضابطاً في القوات الجوية حيث أشرف على العديد من المشاريع المهمة من بينها مشروع «التروبوسكتر والمعدات الملاحية» و«مراكز عمليات القطاع» و«إدارة مراكز الاتصالات في قاعدة الطائف الجوية» وعمل في الفترة من ١٩٩٧م حتى ٢٠٠٢م في رئاسة الاستخبارات العامة إلى أن وصل إلى رتبة لواء مهندس ومساعد لرئيس الاستخبارات العامة للشؤون الفنية، كما عمل خلال سنوات خدمته البالغة ٣٣ عاماً في المجال العسكري، حيث أشرف على العديد من الوظائف الإدارية والفنية بما فيها تطوير وإدارة أنظمة إلكترونية معقدة، من بينها مشروع وصلة ميكروويف رقمية - مشروع اتصالات لاسلكي على مستوى المملكة - مواصفات مقاسم إلكترونية حديثة - مشروع تشفير الفاكس والتلكس. وإنشاء أول هاتف جوال يعمل في المملكة لخدمة كبار المسؤولين ومنسوبي الرئاسة وأشرف على تطويره وإدارته. وقد كان عضواً في عدد من اللجان الرسمية الدائمة أثناء عمله منها: عضو لجنة إعداد ورقة عمل المملكة العربية السعودية لتوزيع الطيف الاستوائي والطيف الترددي مع مندوبين من وزارة البرق والبريد والهاتف ومدينة الملك عبدالعزيز للعلوم والتقنية وعدد من الوزارات والجهات الأمنية والعسكرية. وفي الفترة من عام١٤٠٢هـ إلى عام ١٤٢٠هـ كان عضواً دائماً في لجنة أمن اتصالات الدولة. ومن عام١٤٠٣هـ إلى عام ١٤٢٠هـكان عضواً دائماً في لجنة تراخيص الترددات اللاسلكية. ومن عام١٤١٥هـ إلى عام ١٤٢٠هـ كان عضواً في منظمة الهواتف الجوالة العالمية «GSM». واشترك كذالك في وضع الهيكل التنظيمي لرئاسة الاستخبارات العامة. وتلقى المهندس فريج العويفي تعليمه في المملكة العربية السعودية والمملكة المتحدة والولايات المتحدة الأمريكية، كما شارك في عدد من الدورات وشارك في كثير من المؤتمرات والندوات في مجال الإلكترونيات والتشفير. وحصل على العديد من الأوسمة والميداليات والأنواط منها وسام تحرير الكويت وميدالية التقدير العسكري من الدرجة الأولى، ونوط القيادة ونوط الابتكار ونوط الإدارة العسكرية ونوط الإتقان بالإضافة إلى عدد من شهادات التقدير. وألف المهندس فريج عدد من الأوراق العلمية وكتاب «هندسة نظم الاتصالات» باللغة العربية. بالإضافة إلى كتاب «حروب تقنية المعلومات».

تقديم

فريج بن سعيد العويضي

منذ حوالي ربع قرن تغيرت المفاهيم وتنوعت القضايا، التي تهم المواطنين العاديين والمثقفين والساسة وأصحاب القرار، نتيجة لتغيرات وتطورات كبيرة وسريعة في تقنية نقل وإنتاج وتخزين صناعة المعلومات، نتج عنها تحول كبير في الثقافات وشتى أساليب الحياة. وتحول العالم برمته إلى قرية صغيرة منفتحة ومتواصلة، وأصبحت المعلومات في متناول الجميع؛ وانتقلت ساحات الحروب والمشاحنات وما يحصل فيها من تعديات وظلم وقهر وإذلال للإنسانية بجميع فئاتها وأجناسها وأعمارها إلى صالات المعيشة في كل بيت وفي كل بقعة من العالم في صور حية، تُبث في معظم الحالات فور حدوثها، فالمشاهد الحية، التي يمكن متابعتها من فلسطين المحتلة، أو العراق أو سجون «أبو غريب»، وسجن دلتا في جوانتنامو، وكثيراً مما شابهها من المناظر المزعجة، التي كثيراً ما تغيبها السياسة ويعتم عليها المعتدون؛ أصبحت بفضل الانفتاح الهائل الذي حققته تقنية صناعة المعلومات في متناول الجميع في لحظة وقوعها؛ ومثل هذه الصور والمناظر فعلت ما لم يفعله السحر في إثارة النفوس، وتنمية الحقد والكراهية لدى من يشاهدها. وكلما تفاقم الظلم والقهر واستغلال الشعوب ونهب ثرواتها، ازداد الحقد والرغبة لعمل ما يمكن وما لا يمكن لمنعه. ليس هذا فحسب، بل إن التطور التقني سهَّل سبل الاتصال والتراسل بين جميع فئات المجتمعات، فتشكلت مجاميع

ومنظمات – تعتمد على ما توفره وتسهله التقنية الحديثة – تعمل في شتى مجالات الخير والشر بعضها منظمات خيرية تهدف للصالح العام وتحرير الشعوب بطرق سلمية، وأخرى مهنية تهتم بحقول مختلفة من حقول العلم، والتقنية، والطب، يتبادل أعضاؤها المعلومات ونتائج البحوث والدراسات. أما البعض الآخر فهو منظمات الشر والإرهاب، التي تعمل على نشر فكرة، أو قضية، ترى أنها عادلة حسب مفاهيم المنظمين والمنظرين لها. وقد تكون بالفعل كذلك بصرف النظر عن مشروعية أساليبها، التي قد تنحو منحىً غير إنساني وإجرامي، حيث أنها تكافح لاستعادة حق ضائع أو رد اعتداء من دولة أو عصابة أو منظمات أخرى، فتجد من يتعاطف معها ويدعمها بجميع مستويات الدعم، عندها تبدأ في تجنيد المحاربين وتدريبهم وبث روح الحماس فيهم، وتنظيمهم لينفذوا مهام متعددة الأشكال والنتائج لإرهاب أعدائهم دون الاهتمام بمن سيكون ضمن ضحاياهم من الأبرياء. واحتار المفكرون والساسة ورجال الدين في تعريف هذه المنظمات؛ فهي في نظر البعض دعاة لتحرير الأرض، ورد الظلم، واستعادة الحقوق، وفي نظر الآخرين إرهابيون يهدفون إلى تدمير الحضارة الحديثة وقتل وإرهاب من لا يقر بادعاءاتهم. ومما يؤسف له، أن جميع هذه المنظمات تجد من يستمع لها، ويتعاطف معها، بل وتجد من يضحي بنفسه، في سبيل تحقيق ما آمن به، وسيستمر ذلك، طالما أن هناك عدواناً واحتلالاً للشعوب، وانتشار الفساد بين البشر، واغتصاب المال العام دون وجه حق، وتفشي الظلم، وفقدان العدل.

ومهما كانت الأسباب والتعريفات والمعتقدات؛ فحقيقة الأمر أن البنية التحتية العالمية مهددة، والاختراقات والعبث بالمعلومات المخزنة أو المتداولة من خلال شبكات الاتصال في تزايد مستمر، لأهداف ومسببات شتى شُرحت بإسهاب في ثنايا الكتاب.

و الكتاب، الذي بين يدي القارئ حصيلة خبرة تزيد عن خمسة وعشرين عاماً متواصلة في مجالات الأمن بصورة عامة، وأمن المعلومات على وجه الخصوص، تم التعامل معها عن كثب، وكان من الواجب الأخلاقي والوطني وضعها بين يدي القارئ الكريم، مدعمَّة بما تجمَّع خلال هذه الفترة الطويلة من معلومات تقنية واستخباراتية تتعلق بمكافحة الإرهاب وحماية شبكات الاتصالات بصورة عامة، وشبكات الاتصالات الحكومية على وجه الخصوص، بأسلوب ميسرٍ بعيداً عن التعقيدات الفنية من أجل أن تعم الفائدة.

يتكون الكتاب من ثلاثة أبواب، بدأ الباب الأول بتمهيد لموضوع الكتاب، تم الحديث فيه عن تعريف البنية التحتية والإرهاب وتوضيح اعتمادها بشكل كامل على تقنية صناعة المعلومات، قد يكون مخيفاً. ويضم الباب الأول عدة فصول، يتناول الفصل الأول بدايات الإنترنت وتطورها، حتى وصلت إلى ما وصلت إليه. وفي الفصل الثاني كان من الضروري تقديم نبذة للقارئ الحريص على معرفة تقنيات اختراق الحواسيب وسرقة، أو معرفة ما يخزن فيها من معلومات كتبت بأسلوب ميسر، ليفهمها غير المتخصصين. وطرحت في الفصل الثالث، بنوع من الإسهاب، استخدامات القراصنة والإرهابيين لجميع وسائل التقنية بما فيها الوسائط المتعددة والإعلام الجماعي، والحديث عن بعض مواقع قراصنة المعلومات وإرهابيي الإنترنت واستخداماتهم لتقنية المعلومات المفتوحة والبرمجيات والأدوات المجانية المفتوحة المصدر.

قسّم الباب الثاني من الكتاب إلى ثلاثة فصول، تم تخصيصها للتهديدات، التي تقع على البنية التحتية منذ فجر التاريخ، وحتى هذه الأيام. وتصنيف فشل وإخفاقات الأنظمة، وكيف يفكر القراصنة والإرهابيون؟ ولماذا يمتهنون هذه المهنة غير الأخلاقية؟ وطريقة اختيارهم للثغرات الأمنية. وطرحت أمثلة للعمليات الإرهابية والكوارث الطبيعية وتأثيراتها على الاقتصاد الدولي، وتصنيف مفصَّل عما يُعَدُّ إخفاقات، وأسباب هذه الإخفاقات، وتحديد المخاطر، التي تعترض البنية التحتية. وخصص الباب الثالث والأخير من الكتاب، للحلول والإجراءات الواجب اتباعها لحماية البنية التحتية بجميع عناصرها ومكوناتها، مقسماً إلى فصلين، اشتمل الفصل الأول منه على سبل حماية البنية التحتية، أما الفصل الثاني فهو يوضح المحاور الأساسية لحماية البنية التحتية. معتمداً على خمس محاور تم توضيحها بالتفصيل.

ونظراً لطبيعة موضوع الكتاب التقنية، وجدت أنه من المفيد لمصلحة القارئ غير المتخصص إضافة ملحق (٢)، وهو يحتوي على قائمة المصطلحات وتعريفاتها؛ مع أنني تطرقت لكثير من تعاريف المصطلحات في متن الكتاب.

وختاماً؛ أوجه الشكر والعرفان بالجميل لكل من أسهم في إثراء هذا الكتاب بفكرة أو ملحوظة أو توجيه، أو قدم لي خدمة ساعدت على استدراك بعض النواقص، وإتمام هذا العمل. وأخص بالذكر الأستاذ الدكتور مرزوق بن صنيتان بن تنباك والدكتور أسامة محمد

صالح ألطف الدكتور فايز بن موسى البدراني الحربي على ما أبداه من ملاحظات وتعليقات واستدراكات أفادتني كثيراً، والشكر موصول لأستاذة اللغة العربية المتميزة آمنه العويضي، ولابنتي الدكتورة إلهام على مراجعتهن الدقيقة لمسودة الكتاب.

المؤلف

١٥ سبتمبر ٢٠١٠

الباب الأول

تمهيد: الفضاء الإلكتروني مسرح حروب المستقبل

تمهيد: الفضاء الإلكتروني مسرح حروب المستقبل

قبل عشرين عاماً كنت أتحدث مع صديق أمريكي أستاذ في جامعة دالاس في ولاية تكساس، في أحد فنادق الرياض، وكان التلفيزيون يعرض مباراة لكرة القدم. أما محور الحديث فقد كان يدور حول الظلم، الذي لحق بالفلسطينيين، وكيف أن معظم ضحايا الإرهاب والحروب هم من الأبرياء. وكنا نتمنى أن يكون هناك عدلاً لإنصاف أصحاب الحق ونصرتهم. وأثناء الحديث ارتفعت أصوات الجمهور في التلفزيون بسبب تسجيل أحد الفريقين هدفاً، فنظر إليَّ صديقي وقال مازحاً!! قد يكون الحل أن تجرى مباراة في كرة القدم بين الدول المتنازعة، يتم بعدها تحديد صاحب الحق بناءً على نتائج المباريات. فقلت له: «ولكن من يضمن ألا يهيج جمهور الفريق الخاسر ويبدأ حرباً لا هوادة فيها تحرق الأخضر واليابس، وتقتل الأطفال والأبرياء شيوخاً ونساءً، عندها ينطبق المثل «كأنك يا أبا زيد ما غزيت»».

كانت الإنترنت حينذاك محصورة في الجامعات وبعض الهيئات التعليمية، وكانت تحبو نحو العالمية. وتحول حديثنا إلى الخيال العلمي، وتمنينا لو أن الحروب تتحول إلى برامج تشبيهيه تشرف عليها مجموعة تتحلى بأخلاق عالية وتتميز بالعدل وعدم المحاباة. وكان هدفنا الوحيد من هذا الهزل هو رفع الأسى عن الأبرياء وإبعادهم عن مسرح الحروب. ولم يدر بخلدنا أن هناك فرصة حقيقية لنقل المعارك من المدن والشوارع المكتظة بأناس لا يهمهم سوى لقمة العيش والحياة الكريمة، إلى عالم افتراضي فسيح لا تسيل فيه الدماء ولا تتساقط في أركانه الأشلاء. كانت الإنترنت في بداياتها ولم تتضح معالمها؛ بل أن وسائل الاتصالات لم تكن قادرة

على توصيل المجتمعات ونقل الصور الثابتة والمتحركة بالسرعة والقدرات الممكنة هذه الأيام. ومرت السنون كأنها لمحة بصر ليعيش العالم عصراً جديداً سمي «عصر تقنية المعلومات»، وأصبح العالم الافتراضي جزءاً مهماً من العالم الحقيقي. وأصبحت التقنية جزءاً معتاداً من الحياة، وقد لا يستطيع الإنسان العيش بدونها. وتحكمت تقنية المعلومات في جميع الأمور الاقتصادية والعسكرية والثقافية وسائر أمور المعيشة؛ الأمر الذي أوضح أن حروب المستقبل وتدمير البنية التحتية وشلها، قد تنتقل فعلاً إلى ساحات الفضاء الإلكتروني الفسيح. وتوالت الأمثلة والحوادث، التي أكدت ذلك، من الطرفين ـ الدول النظامية، والمنظمات الإرهابية.

كانت الحرب الإعلامية على أشدها بين الغرب وإيران، عندما انتهت أعمال بناء محطة بوشهر التي بدأت عام ١٩٧٤م بمشاركة مؤسسة/ Kraftwerk Union A.G. Siemens KWU الألمانية. وبعد سنوات من التأخير أعلن «سيرغي نوفيكوف»، الناطق باسم الوكالة الذرية الروسية (روساتوم)، أن روسيا سوف تدشن في ٢١ أغسطس ٢٠١٠م تشغيل المحطة النووية الواقعة جنوب إيران عبر تزويد المفاعل بالوقود، وتم سحب البيان ولم يصدر له أي تصحيح على الفور. ومن المفروض، حسب بيان ورد فيه تصريح لرئيس الوزراء الروسي «فلاديمير بوتين» في ١٨ مارس، أن روسيا تعتزم بدء تشغيل مفاعل بوشهر في صيف عام ٢٠١٠م، وكان واضحاً أن إيران تواجه مشاكل فنية كبيرة. وفي يوليو عام ٢٠١٠م سربت المخابرات الغربية لوكالات الأنباء العالمية خبراً مفاده أن قنبلة إلكترونية ذكية أطلقت لتدمير مفاعل نووي إيراني. ثم توالت تصريحات خبراء أمن الكمبيوتر وتحدثت عن دراسة سلاح إلكتروني جديد، هو قنبلة ذكية عبارة عن فيروس من أخطر ديدان فيروسات الكومبيوتر، ربما يكون قد صمم خصيصاً لتخريب منشأة نووية إيرانية، من قبل دولة - أمريكا أو إسرائيل أو الاثنتين معاً. وقد تكون هذه هي المرة الأولى، التي يتم فيها تطوير دودة فيروسية تستطيع استهداف بنية تحتية حقيقية، مثل محطات الطاقة والمياه والوحدات الصناعية وأجهزة الطرد المركزي. وهذه الدودة الفيروسية تسمى «ستكسنت Stuxnet» صممت بحيث تتعرف على شبكة التحكم في منشأة معينة وتقوم بتدميرها. ويحمل الفيروس بصمات تكنولوجية لنظام تحكم يسعى للعثور عليه، وهو مجهز للعمل تلقائياً في حال عثر على هدفه. وقال جيمس لويس الباحث في مركز الدراسات الاستراتيجية والدولية: «هذا أمر مذهل، يبدو وكأنه يتجاوز عملية تجسس إلكترونية ميسرة». وقد صمم الفيروس خصيصاً لاختراق أنظمة التحكم والحصول على البيانات من إنتاج شركة «سيمنز»، التي تستخدم في

العادة لإدارة إمدادات المياه وحفارات النفط ومحطات الكهرباء وغيرها من المنشآت الصناعية. وينتقل الفيروس عبر بطاقات الذاكرة، من نظام إلى نظام دون الحاجة إلى الإنترنت حسب قوله. ويعد هذا الفيروس «دودة»، لأنه ينتقل من جهاز إلى جهاز ويتكاثر أثناء انتقاله. وفور دخوله جهاز الكمبيوتر الذي يعمل ببرامج «ويندوز»، أو بيئة تشغيل أخرى، يقوم بالبحث عن أي نظام من أنظمة «سيمنز» المبرمجة على الجهاز، التي تدير منشآت مثل التبريد أو تتحكم بسرعة التربينات أو محطات الطرد المركزية. وما أن يجد الفيروس ضالته، حتى يسيطر على الكمبيوتر ويخفي أي تغييرات عن العاملين الذين يشغلونه أو يديرونه، حيث يبدو لهم أن كل شيء على ما يرام، بينما الآلة تقوم بالتحميل الزائد، وتغيير البيانات الفنية، مثل درجات حرارة المفاعل وسرعة دوران الآلات وغير ذلك؛ والهدف النهائي هو التخريب الرقمي.

وأكدت وسائل الإعلام أنه عثر على الفيروس في أنظمة في الهند واندونيسيا وباكستان وغيرها من الدول، ولكن يبدو أن أكبر اختراق له كان في إيران، إذ أن نسبة الاختراق بلغت حوالي ٦٥٪ مقابل ٣٠٪ في دول أخرى. ويتقاطع نمط انتشار الفيروس مع أعمال قامت بها شركة أسندت لها أعمال منشآت نووية.

إن جميع التصريحات والأخبار، التي تناقلتها وكالات الأنباء، تلمح إلى أن الفيروس تم نشره عن طريق الإنترنت، لكن بالنظر إلى تاريخ حروب الشبكات وتقنية المعلومات وبالعودة إلى أواخر حكم «صدام حسين» في بغداد، نجد حدوث هجوم مشابه، لتدمير حواسيب أهم مراكز أبحاث التقنية في العراق إبان تلك الحقبة. كان الموقع العراقي حصيناً للغاية، عجزت المخابرات الغربية والإسرائيلية من الوصول إليه رغم نشرها لعدد كبير من الجواسيس وبدأت تفكر في وسيلة إليكترونية للحصول على معلومات وتدمير كل ما تحتويه الحواسيب والمخازن الإلكترونية من معلومات وبحوث. وهداها تفكيرها الشيطاني إلى معرفة ما يحتاجه المركز من معدات وعلمت عن طريق أحد الجواسيس وبالصدفة، أن المركز يعاني من ارتفاع كبير في حرارة الطابعات المستخدمة. وفوراً اتفقت الاستخبارات مع إحدى الشركات العالمية الشهيرة في صناعة الطابعات ووضعت فيروساً خطيراً في أفضل طابعاتها وأعلنت عنها في المجلات العلمية، التي كان بعض علماء المركز مشتركين فيها. وما أن قرأ العلماء العراقيون الإعلان، حتى وقعوا في الفخ، وسارعوا إلى طلب الطابعة عن طريق شركة وهمية في ألمانيا. وهكذا بدأت مشاكلهم، وتم تدمير معلومات المركز وكل ما يتصل بالطابعة أو الحاسوب المتصل بها.

هاتان الحادثتان ليستا الوحيدتين في هذا المجال، ولكنهما تعدان من أهم ما تم تسريبه إلى الإعلام، وقد يكون الهدف هو إبعاد الشبهة عن الشركات الغربية، التي اشتركت في تنفيذ هذه الحرب الإرهابية. إن علماء إيران، وكذلك علماء العراق، لم يكونوا من السذَّج لربط حواسيبهم المهمة بالإنترنت، ولكنهم كانوا مضطرين لاستخدام أجهزة ومعدات تصنَّع في الغرب. وإذا صحت الإحصاءات المتعلقة بِنسب الاختراق في إيران وغيرها من الدول، المنشورة في وسائل الإعلام، فإن ذلك حتماً قد سُرب كجزء من التمويه والتغطية على الشركات، التي أسهمت في تنفيذ هذا الهجوم. إن العالم اليوم يعيش مرحلة تحول فعلي لحل نزاعاته، ومحاولة سيطرة دولة على أخرى بالاعتماد الكلي على الفضاء الإلكتروني، إذ يمكن لدولة متقدمة في مجال الحروب الإلكترونية وتقنية المعلومات أن تشل دولة أخرى تماماً، وتوقف وسائل مواصلاتها واتصالاتها واقتصادها، بل يمكن أن تعيدها لعصر ما قبل النهضة الصناعية.

وفي هذا الكتاب سيرى القارئ كيف أن دول العالم بدأت تتجه شيئاً فشيئاً نحو الاعتماد على تقنية المعلومات وشبكات الإنترنت لتشغيل بنيتها التحتية بجميع أنواعها. لقد بدأت حروب التقنية ولم تقتصر على قراصنة الإنترنت والمنظمات الإرهابية العالمية، كما سنرى في الفصول التالية، بل إن الدول النظامية بدأت في إنشاء وزارات ومنظمات دفاع وحروب إلكترونية، ونقلت مسارح حروبها إلى الفضاء الإلكتروني الفسيح. أسلحتها قنابل إلكترونية مؤقتة وفيروسات موجهة، وجنودها قراصنة مدربون، ووسائل النقل برامج إلكترونية خاملة توضع في الأجهزة والمعدات المراد بيعها لبقية الدول، أو ترسل عن بعد عن طريق شبكات الاتصالات، أو ينقلها جاسوس أو خائن أو إرهابي إلى حاسوب البنية التحتية المراد تدميرها.

المخاطر المحدقة بالبنية التحتية:

نتيجة للتوجه الجديد في حروب التقنية ـ سواءً من قبل القراصنة والإرهاب الدولي، أو من قبل الدول النظامية ـ فإن العالم يواجه مخاطر كبيرة تهدد سلامة البنى التحتية وفاعليتها. وتعرَّف البنية التحتية في أي بلد بأنها اصطلاح يطلق على كل ما هو متعلق بالمرافق، والنظم، والعلاقات، والمهارات، التي تساعد الدولة على تحقيق أهدافها، وتشمل كافة الخدمات التي لها تأثير مباشر أو غير مباشر على حياة ورفاهية مواطنيها، وكل المقيمين فيها، وتنعكس على المجالات الاقتصادية والتجارية، مثل شبكات الطرق وحركة النقل، والموانئ، والمطارات،

وشبكات المياه، والصرف الصحي، وشبكات الاتصالات، وشبكات الكهرباء، وشبكات نقل النفط، والمدن الصناعية، والمدن المالية، ومناطق التجارة الحرة، وخدمات الإنترنت، والتجارة الإلكترونية، والاتفاقيات والتفاهمات الاقتصادية والتجارية، وسن الأنظمة الإدارية والمالية والقانونية. ونتجت هذه المخاطر من التهديدات الإرهابية العالمية ومن الدول المتقدمة فنياً. ولا يوجد تعريف موحد للإرهاب يتفق عليه جميع السياسيين والقانونيين؛ لأن ما هو إرهاب في نظر البعض يمثل حركات تحررية في نظر الآخرين. فمن منظور الأمة الإسلامية، تم تعريف الإرهاب من قبل المجمع الفقهي الإسلامي، في اجتماعه الذي عقد في ٢٦ شوال ١٤٢٢هـ (الموافق ١٠ يناير ٢٠٠٢م) في رابطة العالم الإسلامي بمكة المكرمة في دورته السادسة عشرة[1]، بأنه «ظاهرة عالمية ، لا ينسب لدين، ولا يختص بقوم، وهو ناتج عن التطرف، الذي لا يكاد يخلو منه مجتمع من المجتمعات المعاصرة. وهو العدوان الذي يمارسه أفراد أو جماعات أو دول بغيًا على الإنسان (دينه ودمه وعقله وماله وعرضه)، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق، وما يتصل بصور الحرابة، وإخافة السبيل، وقطع الطريق، وكل فعل من أفعال العنف أو التهديد، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أحوالهم للخطر. ومن صنوفه أيضاً إلحاق الضرر بالبيئة أو بأحد المرافق والأملاك العامة أو الخاصة، أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر؛ فكل هذا من صور الفساد في الأرض، التي نهى الله سبحانه وتعالى المسلمين عنها في قوله:

﴿وَلا تبغ الْفَسَادَ في الْأَرْضِ إِنَّ الله لا يُحِبُّ الْمُفْسِدِينَ﴾ القصص: ٧٧.

وقد شرع الله الجزاء الرادع للإرهاب والعدوان والفساد وعده محاربة لله ورسوله في قوله الكريم:

﴿إِنَّمَا جَزَاءُ الَّذِينَ يُحَارِبُونَ اللهَ وَرَسُولَهُ وَيَسْعَوْنَ في الأَرْضِ فَسَادًا أَنْ يُقَتَّلُوا أَوْ يُصَلَّبُوا أَوْ تُقَطَّعَ أَيْدِيهِمْ وَأَرْجُلُهُمْ مِنْ خِلافٍ أَوْ يُنْفَوْا مِنَ الأَرْضِ ذَلِكَ لَهُمْ خِزْيٌ فِي الدُّنْيَا وَلَهُمْ فِي الآخِرَةِ عَذَابٌ عَظِيمٌ﴾ المائدة: ٣٣» انتهى تعريف المجمع الفقهي الإسلامي.

ولا يوجد في أي قانون بشري عقوبة بهذه الشدة، نظرًا لخطورة هذا الاعتداء الذي يعد في الشريعة الإسلامية حرباً ضد حدود الله وضد خلقه. وأكد المجمع الفقهي الإسلامي: «أن

من أصناف الإرهاب إرهاب الدولة، ومن أوضح صوره وأشدها بشاعة، الإرهاب الذي يمارسه اليهود في فلسطين، وما مارسه الصرب في كل من البوسنة والهرسك وكوسوفا». ورأى المجمع أن هذا النوع من الإرهاب «من أشد أنواعه خطرا على الأمن والسلام في العالم، وجعل مواجهته من قبيل الدفاع عن النفس والجهاد في سبيل الله».

أما وكالة الاستخبارات المركزية الأمريكية فقد تبنت في عام ١٩٨٠م تعريفًا ينصُّ على أن[٢]: «الإرهاب هو التهديد باستعمال العنف، أو استعمال العنف لأغراض سياسية من قبل أفراد أو جماعات، سواء تعمل لصالح سلطة حكومية قائمة أو تعمل ضدها، وبخاصة عندما يكون القصد من تلك الأعمال إحداث صدمة، أو فزع، أو ذهول، أو رُعْب لدى المجموعة المُسْتَهدَفَة، التي تكون عادة أوسع من دائرة الضحايا المباشرين للعمل الإرهابي. ويشمل الإرهاب جماعات تسعى إلى قلب أنظمة حكم محددة، وتصحيح مظالم محددة، سواء كانت مظالم قومية أو لجماعات معينة، أو بهدف تدمير نظام دولي كغاية مقصودة لذاتها». والتعريف الأخير مصاغ لإدخال منظمات المقاومة الوطنية والتحررية، مثل المقاومة الفلسطينية وما شابهها في دائرة الإرهاب وإخراج ما تمارسه إسرائيل ضد الفلسطينيين.

وقد ساعد التطور التقني، الذي شهده هذا العصر، في تهيئة تسهيلات كبيرة للإرهابيين، رغم أنه أدى إلى نشوء إمكانيات جديدة لتطوير الخدمات وخفض التكاليف ورفع الكفاءة. ونتيجة لهذا التطور تحول العالم إلى أمم مترابطة سلكياً ولا سلكياً لتصبح في وضع معقد لا يمكن تصور ما سيئول إليه مستقبلاً.

وفي السنوات القليلة الماضية، تطور «التحكم الحاسوبي»، أو مكننة وأتمتة البنية التحتية على مستوى العالم. «والأتمتة: مصطلح جديد مأخوذ من الكلمة الإنجليزية Automation»؛ وتعني تنفيذ أي عملية بواسطة أنظمة تحكم آلية ودون تدخل الإنسان، حيث تقوم هذه الأنظمة بتشغيل خطوط الإنتاج، ونظام التحكم فيها وبمنظوماتها العامة، والتحكم بالعملية الإنتاجية بالكامل. أما المكننة فهي استبدال عمل الإنسان بعمل الآلة، وعادة ما يكون ذلك في الأعمال الإدارية اليدوية، مثل توزيع المعاملات أو التعاميم، والتقارير، والمراسلات الإدارية، وتوزيع الرواتب، وضبط الإجازات بين جميع إدارات وأقسام المصلحة، عن طريق نظام تحكم حاسوبي يعمل من خلال برامج مجمعة

ومترابطة تم تصميمها حسب أنظمة المؤسسة أو المصلحة، حيث تقارن البرامج وتحسب وتستنتج وتوزع جميع المتطلبات حسب الوظائف المعتمدة فيها. ويمكن القول أن النمو المستمر المتعلق بإنتاجية العمل يركز في الوقت الحالي وبالدرجة الأولى على مكننة الأعمال اليدوية، وأتمتة العمليات الإنتاجية، وتتجه الأعمال في مجال المكننة والأتمتة إلى الانتقال إلى الأتمتة الشاملة، وإلى إيجاد أقسام وورش ومصانع مؤتمتة بالكامل، وتدخل المكننة والأتمتة الشاملتين، في أكثر فروع الإنتاج حجماً للعمل، مثل إنتاج المسبوكات، وصناعة السيارات وطرق نقل المواد من مكنة إلى أخرى في خطوط الإنتاج وفي مجالات التشغيل الميكانيكي والعمليات الإنتاجية التسلسلية في المصانع الكبيرة.

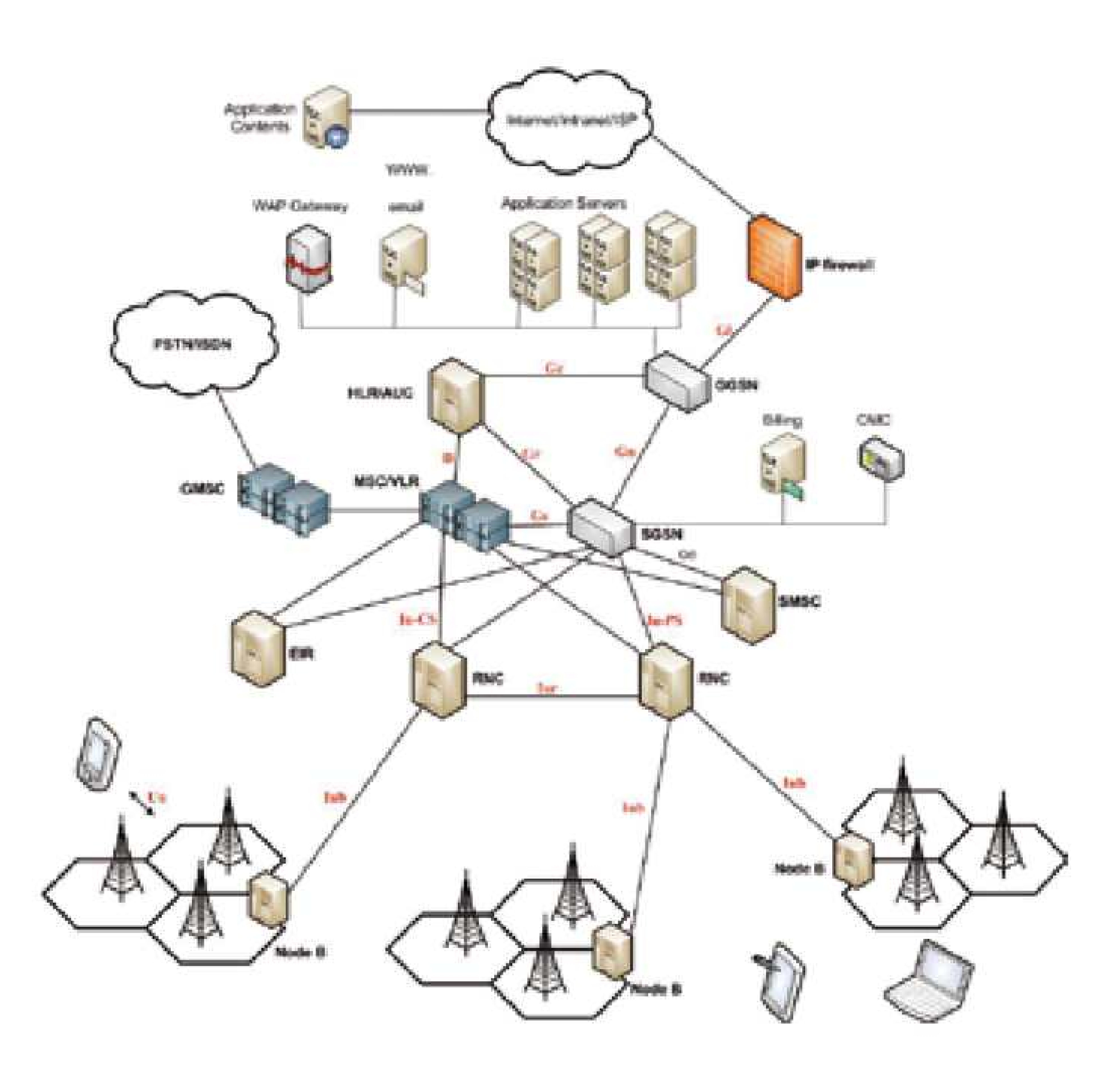
وقد شمل هذا التطور المدهش والمتسارع، جميع القطاعات مثل المواصلات والنقل والتعاملات المالية وقطاع الطاقة وقطاع الاتصالات، واقترن بالتوازي مع التطور السريع في تقنية الحواسيب والمعلومات والشبكات، مما فتح المجال واسعاً أمام الإرهاب الدولي ومكّنه من الوصول إلى مكونات البنية التحتية. ومن الضروري أن يعي العالم أجمع، أهمية استمرارية وسلامة عمل مكونات البنية التحتية، ومعدات مكننتها الآلية، وعناصرها التقنية، من برامج وآلات وأدوات، بفعالية وموثوقية واعتمادية واستمرارية عالية.

ويستخدم اصطلاح «الاعتمادية» بأسهل معانيه للتعبير عن عمليات سليمة خالية من العيوب يمكن الاعتماد عليها بموثوقية عالية من منظور المستفيد من الخدمات ومقدمها، على الرغم من وجود بعض التحديات المعقولة. أما الموثوقية فهي تعبر عن مدى صحة وسلامة المعلومات وضمان حمايتها من التغيير أو التزوير أو الفقدان، بحيث يمكن الوثوق في محتواها وجودة خدماتها والاعتماد عليها بصورة مستمرة، وذلك بضمان عمل جميع أنظمة ومكونات البنية التحتية، التي أصبحت من ضروريات الحياة للعالم أجمع.

والسؤال المهم، الذي يطرح نفسه هو: هل تستشعر حكومات العالم والأسواق العالمية خطورة القصور والعجز الجزئي أو التام في أنظمة البنية التحتية بما فيه الكفاية، وتعمل بجد للحد من أسبابها وتعزز اعتماديتها وموثوقيتها؟ أم أن العالم ينتظر حدوث كارثة كونية في بنيته التحتية الحديثة ليعمل ما يمكن عمله؟ وحتى الآن يمكن اعتبار البنية التحتية في العالم قوية لدرجة مقبولة، وأن أي قصور قد حدث حتى الآن لا يتعدى كونه مزعجاً وليس كوارثياً.

ولكن ليس هناك ما يطمئن إلى أن الأعطال المستقبلية ستكون محدودة، ولن ينتج عنها كوارث على المستويات الأمنية والاقتصادية والصحية.

شكل رقم(١): شبكة نقل معلومات نموذجية



فخدمات البنية التحتية في العالم تعتمد إلى حد كبير وبأسلوب متزايد على شبكات نقل المعلومات، مثل شبكات الاتصالات التي تشمل الكوابل المحورية والاتصالات الفضائية والهواتف الثابتة والنقالة وشبكات نقل الطاقة وتشمل شبكات الكهرباء وشبكة أنابيب الغاز وأنابيب نقل النفط؛ وجميع هذه الشبكات ممكننة إلى حد ما حالياً، وفي اتجاه شامل ومتزايد

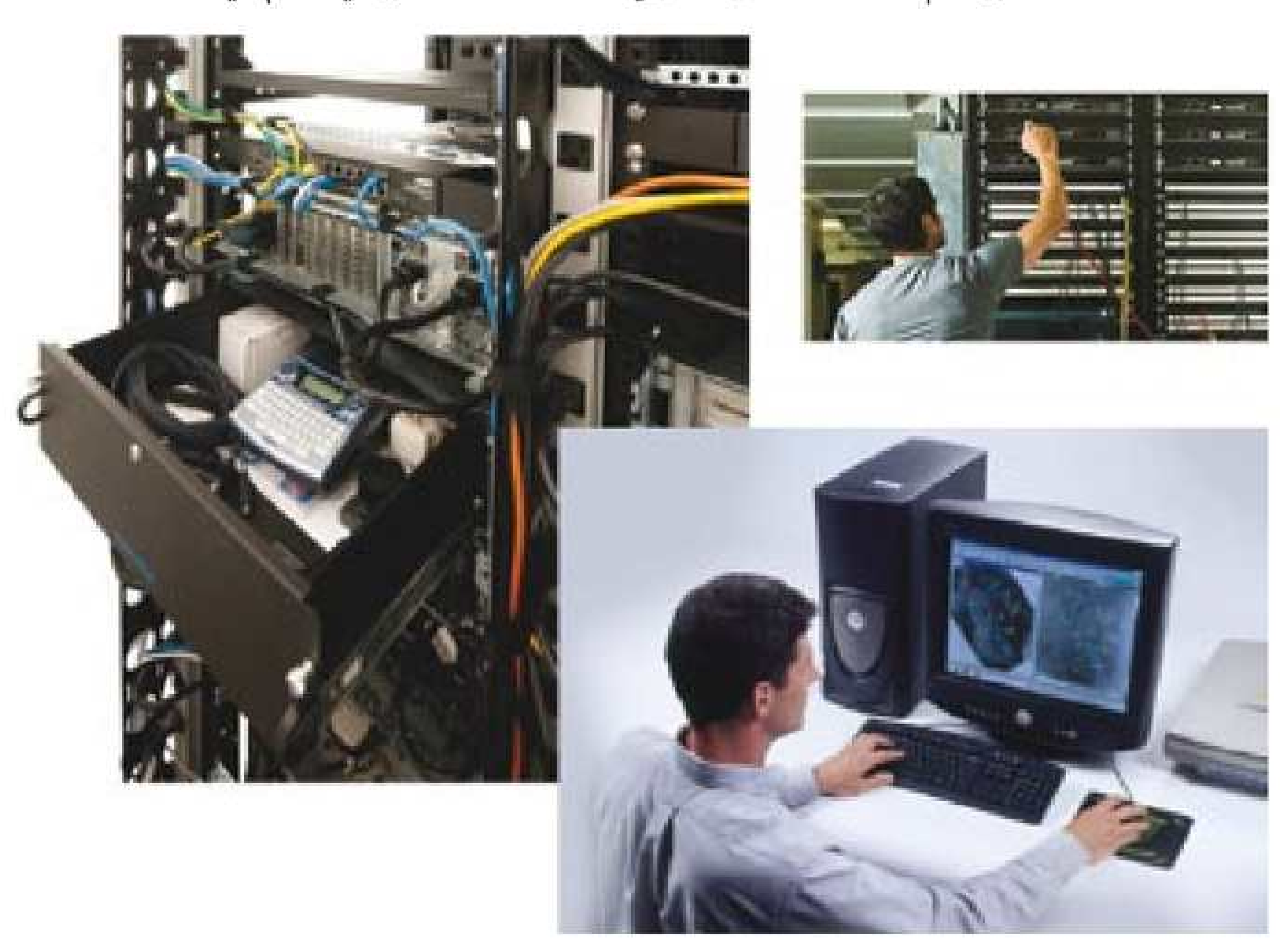
نحو مزيد من الاعتماد على التحكم الحاسوبي لتنفيذ جميع وظائفها التشغيلية مما جعل احتمالية تعرضها للأعطال والتخريب عالية جداً.

كما أن بيئة العمل تغيرت لتعمل بتشريعات وقيود تنظيمية غير محكمة، وأصبحت مفتوحة أمام المستخدمين في شتى أنحاء العالم بتكاليف منخفضة، وارتفاع كبير في المنافسة، بالإضافة إلى سهولة دخول شركات جديدة إلى السوق لتقديم خدمات البنية التحتية بتزايد وتسارع واضح. كما أصبح من السهل الدخول عن بعد إلى جميع قطاعات البنية التحتية الممكننة وشبكات نقل المعلومات، التي تدعم البنية التحتية، رغم زيادة القرصنة والتطفل والاقتحام على الأنظمة، الذي أصبح شائعاً ومعقداً. وتعد شبكات نقل الطاقة وشبكات نقل المعلومات وأي قطاع من قطاعات البنية التحتية الممكننة نقطة ضعف مميتة لأي أمة؛ لأنها تشكل عصب الثروات والوظائف اليومية، ومع ذلك فهي ليست حصينة، وهي معرضة للهجوم والاختراقات المؤثرة. ولا يستغرب أن تتركز جهود الجيل القادم من الإرهاب الدولي على محاولة تدمير البنية التحتية العالمية. ويمكن القول أن تعطيل أو عزل عدد قليل من نقاط شبكات نقل المعلومات أو الطاقة يمكن أن تتسبب في تعطيل كامل الشبكة، وذلك بسبب تقسيم الشبكة إلى جزر معزولة عن بعضها. وتؤكد كثير من الدراسات التحليلية للشبكات الديناميكية على وجه الخصوص (وهي الشبكات، التي تتغير أحمالها وتتعرض سرعة نقل المعلومات من خلالها للتغير المستمر) على وجود طرق أسهل لتدميرها، تتمثل في الأعطال التسلسلية، وسيتم شرح ذلك بالتفصيل لاحقاً.

إن البنى التحتية القائمة اليوم، أو التي تحت الإنشاء في جميع دول العالم، تحدد توجه ومستقبل الاقتصاد الوطني في تلك الدول، كما أن اعتماد المجتمع في التعاملات اليومية، على الشبكات الإلكترونية يتزايد بسرعة هائلة؛ فخدمات قطاع المواصلات، وقطاع النقل، وقطاع الطاقة، وقطاع المال، وقطاع الاتصالات، وشبكات الحواسيب، أصبحت من ضروريات الحياة، وهي خدمات أساسية لا يمكن الاستغناء عنها. وبمجرد النظر في آليات وأدوات التحكم في الملاحة الجوية المسؤولة عن سلامة آلاف الرحلات الجوية يومياً، والتعاملات المالية التي تقدر ببلايين الريالات في كل يوم، وإشارات التحكم في تشغيل الشبكة العامة للكهرباء، وأنابيب البترول وأنظمة الهاتف الثابت والجوال، يظهر بوضوح أن كل ذلك ينقل على شبكات المعلومات المحلية والعالمية السلكية أو اللاسلكية، فنظام شبكات نقل المعلومات الإلكترونية

يمثل النسيج العصبي، الذي ينمو ويتضاعف بسرعة فائقة في صميم تقنية المعلومات، التي تميز عالم اليوم. والأسئلة، التي يمكن طرحها هذه الأيام، إلى أي مدى يمكن الاعتماد على هذه الشبكات؟ وكيف يمكن التأكد من موثوقية محتواها واعتماديتها بما فيه الكفاية؟

شكل رقم(٢): العنصر البشري جزء لا يتجزأ من أي نظام آلي



فالبنية التحتية التي يمكن الاعتماد عليها هي التي تصمم بطرق تجعل من المستحيل أو الصعب تدميرها بصورة شاملة، كما يمكن إعادتها لحالتها الطبيعية في وقت مقبول وبخسائر معقولة، وليس من السهل الإجابة عن هذه الأسئلة، فبنية منظومة الاتصالات والشبكات الممكننة شديدة الحساسية، وتواجه تحديات حقيقية من التهديدات الطبيعية إلى الأخطاء الإنسانية، ومن أعطال الأجهزة إلى أعمال الإرهاب والقرصنة.

من المنظور الفني الخالص وبعيداً عن الاعتبارات القانونية يمكن استخلاص أن جميع هذه التهديدات متساوية؛ فهي أوجه مختلفة لمشكلة واحدة. وتكمن أهم الأمور الإجرائية لمواجهة وإدارة هذه المخاطر والتهديدات في حصرها وتحديد الثغرات الفنية لكل جزء من أجزاء النظام والخروج بتحليل فني دقيق يؤدي إلى اتخاذ إجراءات هندسية مستدامة لتعزيز

الاعتمادية والموثوقية. ومهما بلغت مقدرة أدوات التقنية لتعزيز الاعتمادية، فلن تكون الجواب الفعال لهذه التهديدات. فاعتمادية التقنية بصورة عامة، وتقنية المعلومات على وجه الخصوص، يمكن فهمها جيداً لو وضعت في سياقها الاجتماعي؛ لأن الأشخاص يمثلون الحلقة القوية وكذلك الحلقة الضعيفة في سلسلة الاعتمادية؛ لذا يجب عدم الغفلة عن العنصر البشري عند حصر التحديات التقنية لضمان اعتمادية البنية التحتية. وقد يكون من أهم الخطوات الأساسية لتلافي مشاكل الاعتمادية الحرص على تنمية ثقافة الحذر واليقظة في المجتمع، وعند تحديد حجم ومستوى الاعتمادية التي تحتاجها الشبكات الداعمة للبنية التحتية ضد أي من التهديدات، وعندما يحدد مقدار التكاليف الواجب رصدها، يجب وضع ذلك ضمن نسيج السياسات العامة، التي تحتاج إلى متابعة دائمة من ملاك التقنية ومقدمي الخدمات في كامل المجتمع والدولة. والهدف الرئيس من هذا الكتاب هو محاولة توضيح التهديدات، التي تعترض البنية التحتية، سواءً الناتجة عن الكوارث الطبيعية، أو التي يتسبب فيها الإنسان بوعي أو دون وعي، وتوضيح الأهداف والمحاولات الإرهابية المتزايدة والتخطيط لها، بالإضافة إلى جعل الكتاب وسيلة متواضعة لتثقيف المهنيين والمهتمين بتقنية المعلومات ممن ينقصهم الوعي الأمني الكامل، وتحديد المتربصين بالمستفيدين والمستخدمين للأنظمة وبمعلوماتهم وخططهم وماذا يفعلون للوصول إليها، ومحاولة تأسيس الخطوط الرئيسة للمعرفة الأمنية. كما أنه يهدف إلى دق ناقوس الخطر لجميع المسؤولين بمختلف مستوياتهم، وستشمل دائرة أمن تقنية المعلومات المشغلين، الذين يمثلون أقصى المخاطر في هذه الأيام، وهم المستخدمون الشرعيون غير الواعين. إن ظاهرة الإنترنت قد تجاوزت مرحلة كونها ظاهرة ترفيه، وأصبحت عنصراً أساسياً من عناصر الحياة، وصارت تؤدي دوراً كبيراً في حياة الشعوب والمجتمعات المدنية اليومية، واعتمد العالم بأسره عليها، حتى أصبحت أداة لا غنى عنها لتسيير جميع خدمات البنية التحتية في العالم. ولكون الكتاب موجه لأكبر شريحة في المجتمع؛ فإنه قد يكون من الضروري توضيح نقاط ومكامن الضعف في مكونات البنية التحتية بأسلوب ميسر؛ حيث يشرح بنوع من التفصيل طرق مهاجمة الأنظمة، وأنواع الهجوم والوسائل والأدوات، التي يستخدمها قراصنة الشبكات بجميع أنواعهم وفئاتهم، ومن المسلّمات، التي أثبتها التاريخ القديم والمعاصر، أن أي تطوير يهدف لتسهيل الخدمات العامة في أي مجتمع، من الضروري أن يكون مفتوحاً ومتيسراً لكامل شرائح المجتمع من أخياره وأشراره، وليس من الواقع العملي تطوير أي قطاع لخدمة المجتمع وجعله حكراً على الأخيار. وهناك علاقة بين تقدم التقنية

والاعتماد عليها للتحكم في البنية التحتية العالمية، وتوجه العالم لفتح أساليب التحكم في بنيته التحتية. ورغم ما يسببه الانفتاح التام على قطاعات البنية التحتية من مخاطر، خاصة في هذا العصر الذي تزايدت فيه المنظمات الإرهابية؛ فإنه أمر لا مناص من تحقيقه. إن تأثير الإرهاب الدولي على الاقتصاد العالمي واضح، وهو نتيجة حتمية لما يقوم به من محاولات تدميرية للبنية التحتية العالمية، الأمر الذي يزيد من خطورة المنظمات الإرهابية على البنية التحتية. والضرر الذي يمكن أن يسببه الإرهاب في عناصر البنية التحتية العالمية، مثل قطاع الاتصالات والكهرباء والاقتصاد والمواصلات ليس سهلاً، كما أن طرق الحماية من الاختراقات موضوع في غاية الصعوبة والتعقيد. وحتى يعيش العالم في رفاه ويسر؛ من الضروري الاهتمام بوضع الحلول وتقديم التوصيات والاستنتاجات والتركيز عليها لحماية شبكات المجتمعات العالمية وإنجازات العالم التقنية.

الفصل الأول

الفضاء الإلكتروني الفسيح

الفصل الأول

الفضاء الإلكتروني الفسيح

هناك فارق بين الإنترنت والشبكة العنكبوتية «WWW»، فالإنترنت عبارة عن توصيل أنظمة الشبكات، التي تمكن الحواسيب من التواصل الآلي، باستخدام نمط التحكم في الإرسال وبرتوكول الإنترنت TCP/IP، وقد تسببت الإنترنت في ولادة الشبكة العنكبوتية العالمية، التي تمثل مجموعة الوثائق الكاملة المخزنة في جميع الحواسيب المنتشرة في الفضاء العالمي وتستخدم نمط HTTP. ويمكن الوصول إلى هذه الوثائق من خلال متصفح الشبكة Browser، بالإضافة إلى التنقل بين الصفحات باستخدام روابط تطبق لغة HTML. وباختصار يمكن تعريف الشبكة العنكبوتية بأنها الشبكة، التي توصل الحواسيب بالصفحات والملفات، التي تعوَّد المجتمع على تصفحها.

تاريخياً ظهرت الإنترنت قبل الشبكة العنكبوتية بسنوات طويلة إذ بدأت الإنترنت عندما قررت وزارة الدفاع الأمريكية إنشاء شبكة معلومات في عام ١٩٦٩م من خلال تمويل مشروع من أجل ربط الإدارات المعنية في الوزارة مع متعهدي القوات المسلحة، وعدد كبير من الجامعات، التي تعمل على أبحاث ممولة من قبلها، وسميت هذه الشبكة باسم (أربا) ARPA اختصاراً للجملة الإنجليزية The Advanced Research Project Administration. وكان الهدف من هذا المشروع تطوير تقنية تشبيك حواسيب تصمد أمام هجوم عسكري[٣].

وصممت شبكة « أربا» باستخدام أداة: «إعادة التوجيه الديناميكي Dynamic rerouting»، ويمكن لهذه الأداة أو الوسيلة تشغيل الشبكة بشكل مستمر، حتى في حالة انقطاع إحدى الوصلات أو تعطلها عن العمل، حيث تنقل الحركة إلى وصلات أخرى .

أما الشبكة العنكبوتية فلم تظهر إلا مع بداية عام ١٩٩٠م، وقد أثار نموها السريع الدهشة. ونظراً لهذا التطور السريع، والانفتاح الذي تسببت فيه تقنية الشبكة العنكبوتية؛ تمكنت الشبكة العالمية المفتوحة من الاستحواذ على مسمى «الإنترنت». إذ اصطلح على تسمية الشبكات الخاصة مثل شبكة «أربا» وشبكات الشركات الخاصة المعزولة بمصطلح «الإنترانت». أما الشبكات العالمية المفتوحة فقد أخذت مسمى «الإنترنت»، وهو المصطلح الذي سيتم استخدامه في هذا الكتاب. وخرجت الإنترنت من غمرتها النسبية، كأدوات للبحث ومعالجة المواضيع العلمية في الجامعات ومراكز البحوث، إلى الدور الكبير، الذي تلعبه هذه الظاهرة اليوم، كوسيلة رائجة وسهلة الاستخدام ومنخفضة التكاليف، لتبادل المعلومات والحصول عليها والتواصل الاجتماعي والتجاري ونشر الثقافات.

إن الإنترنت شبكة عالمية يتم من خلالها توصيل آلاف الشبكات الحاسوبية المختلفة، من حيث النوع والبيئة التشغيلية، بملايين الحواسيب العامة والشخصية المنتشرة حول العالم. وعن طريق الإنترنت، يزاول ملايين الناس أعمالهم اليومية، وملايين آخرون يستخدمونها للمتعة والتواصل مع الآخرين، ليس هذا وحسب، بل إن الإنترنت تسببت في ظهور ثقافات جديدة ودعمت أسواق كان من المستحيل ظهورها، دون التطور المتزايد في وسائل الاتصالات، والقدرات الواسعة في صناعة الحواسيب وأدوات التراسل. إذ أُطلق على الأسواق الجديدة الناشئة «الأسواق الافتراضية Non Market». وهي تنمو بتسارع كبير، وتعتمد على الإنترنت في تعاملاتها.

أما تأثيرها على الاقتصاد العالمي فقد كان جوهرياً، حيث تعرض لتغيرين متوازيين أديا إلى تأرجح واضح في الأنظمة والقيود، التي تتحكم في تسويق المنتجات وتعاملات الأسواق التقليدية، فأثرت على القيم السوقية، التي تمارسها المجتمعات الحرة:

التغيير الأول:[٤] هو الذي بدأ يظهر منذ أكثر من قرن، على هيئة اقتصاد يتمحور حول المعلومات (خدمات مالية، محاسبية، برمجيات، علوم)، وخدمات ثقافية (أفلام،

موسيقى)، وتشكيل الرموز والشعارات التجارية (بدءاً من صناعة أحذية الرياضة مثلاً إلى تسجيل علامتها التجارية، وصناعة الأهمية الثقافية للألعاب الرياضية المستخدمة لتلك الأحذية).

أما التغيير الثاني، فقد سلك اتجاه بيئة مبنية على ظهور معالجات إلكترونية منخفضة الثمن لها قدرات حسابية عالية وتوصيلها بشبكات اتصال تغطي العالم بأكمله اصطلح على تسميتها: «ظاهرة الإنترنت»، نتج عنها دور متزايد للأسواق الافتراضية في قطاع إنتاج المعلومات والثقافة وتنظيمه على أساس اللاملكية، وفق طراز قد يكون مستحيلاً في القرن العشرين.

ويعني التغيير الأول أن الأسلوبين الجديدين للإنتاج عن طريق الأسواق الافتراضية واللاملكية سينشئان في جوهر الاقتصاد المتطور، ولن يكونا على حافته. والواضح أن الإنتاج الاجتماعي التعاوني، الذي يعتمد على اللاملكية والمتاجرة، سيؤديان دوراً أكبر من أي وقت سابق في الثقافات والديمقراطية الحديثة والعدالة الاجتماعية، مقارنه بما حققته العقارات ومنتجات الأسواق التقليدية.

لقد تضاعف استخدام الإنترنت عدة مرات خلال السنوات القليلة الماضية، ويقدر عدد المستخدمين للشبكة على مستوى العالم بـ:١,٧٣٣,٩٩٣,٧٤١ (أكثر من بليون ونصف) مستخدم حسب إحصائيات الإنترنت العالمي[٥] في ٢٩ ديسمبر عام ٢٠٠٩م. كما تسارع النمو في وسائل الاتصال بمعدلات هائلة، حيث تضاف شبكة واحدة كل ٣٠ دقيقة. ولأن شبكة الإنترنت تسعى لأن تكون شبكة متجانسة ومترابطة، فمن المستحيل عملياً معرفة أين تنتهي شبكة ما، وأين تبدأ الأخرى. وتمشياً مع هذا التطور نفذت معظم الدوائر والوزارات في العالم، برامج تقنية طموحة في مجالات تقنية المعلومات، وأنشأت بيئة فاعلة في مجال التعاملات الإلكترونية نتج عنها تشغيل عدد من الشبكات ذات النطاق العريض. ودخلت خدمات الإنترنت في المملكة العربية السعودية للمرة الأولى في عام ١٩٩٤م، عندما حصلت المؤسسات التعليمية والطبية والبحثية على تصريح بالدخول إلى شبكة الإنترنت. أما التشغيل الرسمي العام لشبكة الإنترنت في المملكة فقد كان في عام ١٩٩٧م بموجب قرار وزاري[٦]، حيث فتح المجال للعامة بالوصول إلى الشبكة العالمية في عام ١٩٩٩م.

بلغ عدد مستخدمي الإنترنت في المملكة في شهر ديسمبر لعام ٢٠٠٠م حوالي ٢٠٠,٠٠٠ مستخدم، ازداد هذا العدد، حتى وصل إلى ٢,٥٤ مليون مستخدم في عام ٢٠٠٥م، مما يعني نمواً بنسبة ١١٧٠٪، إذ تعد المملكة أحد أسرع الأسواق العالمية نمواً في هذا القطاع[٧]. وفي عام ٢٠٠٦م، تم إدخال عدد من التغييرات الرئيسة على نظم وسمات خدمات الإنترنت في معظم دول العالم، ومن المرجح أن تسهم هذه التغييرات في توسيع استخدامات الإنترنت، نتج عنه أن بلغ عدد مستخدمي الإنترنت في المملكة العربية السعودية ٧,٧٦١,٨٠٠ في سبتمبر ٢٠٠٩م. وتشير التوقعات إلى مواصلة نمو استخدامات الإنترنت في المملكة.

إضافةً إلى بنية الإنترنت الجديدة، التي من شأنها خفض أسعار استخدام الإنترنت، ثمة عوامل أخرى من شأنها تعزيز نمو استخدامات الإنترنت في المملكة العربية السعودية. ومن أهم تلك العوامل نمو التركيبة السكانية الشابة في المملكة، حيث إن ٦٠٪ من عدد السكان في عمر أقل من ١٨ عاماً، وهذه الشريحة يمكنها التعامل مع التقنيات الحديثة أسرع مما هو متوقع. ومع نمو استخدامات الإنترنت في جميع الدول العربية، ستتزايد باضطراد كمية المحتويات العربية على الإنترنت، مما يشكل عامل جذب أكبر للسعوديين لاستخدامها. كما أن العديد من الجامعات والكليات في المملكة تتبنى حالياً أساليب التعليم الإلكتروني كجزء من مناهجها الدراسية.

ويتوقع نمو سوق التعليم الإلكتروني في المملكة بنسبة ٣٣٪ سنوياً على مدى الخمس سنوات القادمة، وقد تصل قيمته حسب التوقعات إلى ١٢٥ مليون دولار في عام ٢٠٠٨م، ونظراً لأن المزيد من البنوك والشركات ستقدم المزيد من خدماتها عبر الإنترنت، فسيزداد عدد العملاء الذين يستخدمون هذه الخدمات، ومن المتوقع أن تتجاوز قيمة التجارة الإلكترونية في دول مجلس التعاون الخليجي مبلغاً قدره بليون دولار أمريكي مع حلول عام ٢٠٠٨م، وتحصل المملكة العربية السعودية على حصة الأسد من هذه الإيرادات.

كنتيجة لهذا التطور السريع في تقنية الحواسيب، اتجهت معظم الوزارات والمؤسسات المالية والتجارية والأمنية والمؤسسات الخاصة والتعليمية، للاعتماد لأقصى حد ممكن على أنظمة المعلومات ذات التحكم الآلي، وهذه الأنظمة بدورها تزايد ربطها عالمياً لتكّون مجموعات مرتبطة ببعضها لتصبح جزء من الفضاء الإلكتروني الضخم. وكثير من الوزارات والمؤسسات

الحكومية بما فيها الدفاعية والأمنية والمؤسسات المالية تستخدم شبكة الإنترنت لتبادل الرسائل الإلكترونية أو الدخول لحاسوب خارج موقع الوزارة أو المؤسسة وربما خارج الدولة، مثل السفارات ومكاتب الخطوط وغير ذلك، وكذلك تستخدم الإنترنت لتحميل ملفات من وإلى الشبكة على مستوى العالم.

لقد أثبتت الحروب التي خاضتها الولايات المتحدة حول العالم أن القوات المسلحة الأمريكية ومخابراتها المركزية والعسكرية تعتمد إلى حد كبير على شبكات الإنترنت لتناقل المعلومات الحساسة بما فيها المعلومات الاستخباراتية ومعلومات مكافحة التجسس مع حلفائها حول العالم وخبرائها في وزارة الدفاع الأمريكية[٨]. ويعتقد الخبراء العسكريون أن القوات الأمريكية ستزيد من اعتمادها على شبكة الإنترنت في المستقبل، ويعتقدون كذلك أن الرسائل عن طريق الإنترنت، التي ترسل من منطقة النزاع، توفر إنذاراً مبكراً عن التطورات المؤثرة قبل أن تصل المعلومات بالطرق التقليدية، التي قد تكون متأخرة وتنتهي فائدتها، بسبب التأخير الناتج من الحرص على ضمان سريتها. بالإضافة إلى أن الإنترنت يمكن أن تستخدم كوسيلة احتياطية للتراسل أثناء النزاعات والحروب. وللإنترنت دور كبير وجوهري في حرية النمو الإنساني، يتعلق بالدور الذي توفره المعلومات والمعرفة والثقافة وطريقة إنتاجها وتداولها للمجتمعات الإنسانية، فهي تؤثر بعمق في رؤيتنا للحالة الآنية لعالمنا الحاضر ومستقبله، ومعرفة من يقرر كيف يسير عالمنا وإلى أين يتجه، وكيف يمكن لنا كمجتمعات وحكومات أن نستوعب ما يمكن فعله.

أما فيما يتعلق بالثقافات الاجتماعية والديمقراطية، فإنها بكل تعقيداتها اعتمدت لأكثر من قرن ونصف على الاقتصاد المعرفي وصناعة المعلومات، لتحديد العناصر والأدوار الأساسية التي تلعبها المجتمعات[٤]. عندما ظهر تحول جذري في نظم إنتاج المعلومات خلال الخمسة عشر عاماً الماضية، بسبب التطور التقني السريع، أدى إلى ظهور متواليات من التكيف الاقتصادي والاجتماعي والثقافي، نتج عنه تحول جذري في وسائل السيطرة على بيئة معلومات مستقلة، يتحكم فيها الأفراد المستقلين وأعضاء المجموعات الثقافية والاجتماعية، مما كان له تأثير على تقريب الثقافات العالمية، والتوجه نحو خلق ثقافة عالمية تقبل جميع الثقافات على اختلافها وتنوعها وغرابتها، وربما ليس من المستحيل صهر عدد كبير من الثقافات العالمية في ثقافة واحدة تقبل جميع الثقافات.

إن الحديث عن الثورة، التي أحدثتها الإنترنت هذه الأيام ، ليس جديداً إذ تنظر إليه بعض الدوائر العلمية على أنه حصيلة حاصل غير جدير بالنقاش، ومن المفروض ألا يكون كذلك، فالتغيير، الذي أو جدته بيئة الإنترنت عميق وهيكلي، لأنه يتصل بأساس التطوير المشترك بين حرية الديمقراطية والأسواق الافتراضية. وقد أدت التغييرات المتتالية في التقنية والمنظمات الاقتصادية والممارسات الاجتماعية للإنتاج من خلال تلك البيئة، إلى ظهور فرص جديدة لوسائل إنتاج وتبادل المعلومات والمعرفة والثقافة على مستوى عالمي، وأدت هذه التغيرات بدورها إلى زيادة دور منتجات الأسواق الافتراضية، وهي المنتجات التي لا تخضع للملكية الخاصة، من خلال جهود فردية وجهود تعاونية في مجال واسع من نسيج متماسك، كما يحصل في الجامعات ومراكز البحوث، ونسيج غير متماسك، كما هو حاصل في بيئة الإنترنت، حيث يتعاون عدد كبير من الناس المنتشرين في شتى أنحاء العالم لحل كثير من المشاكل التقنية وتبادل المعلومات دون أي رابط يجمعهم.

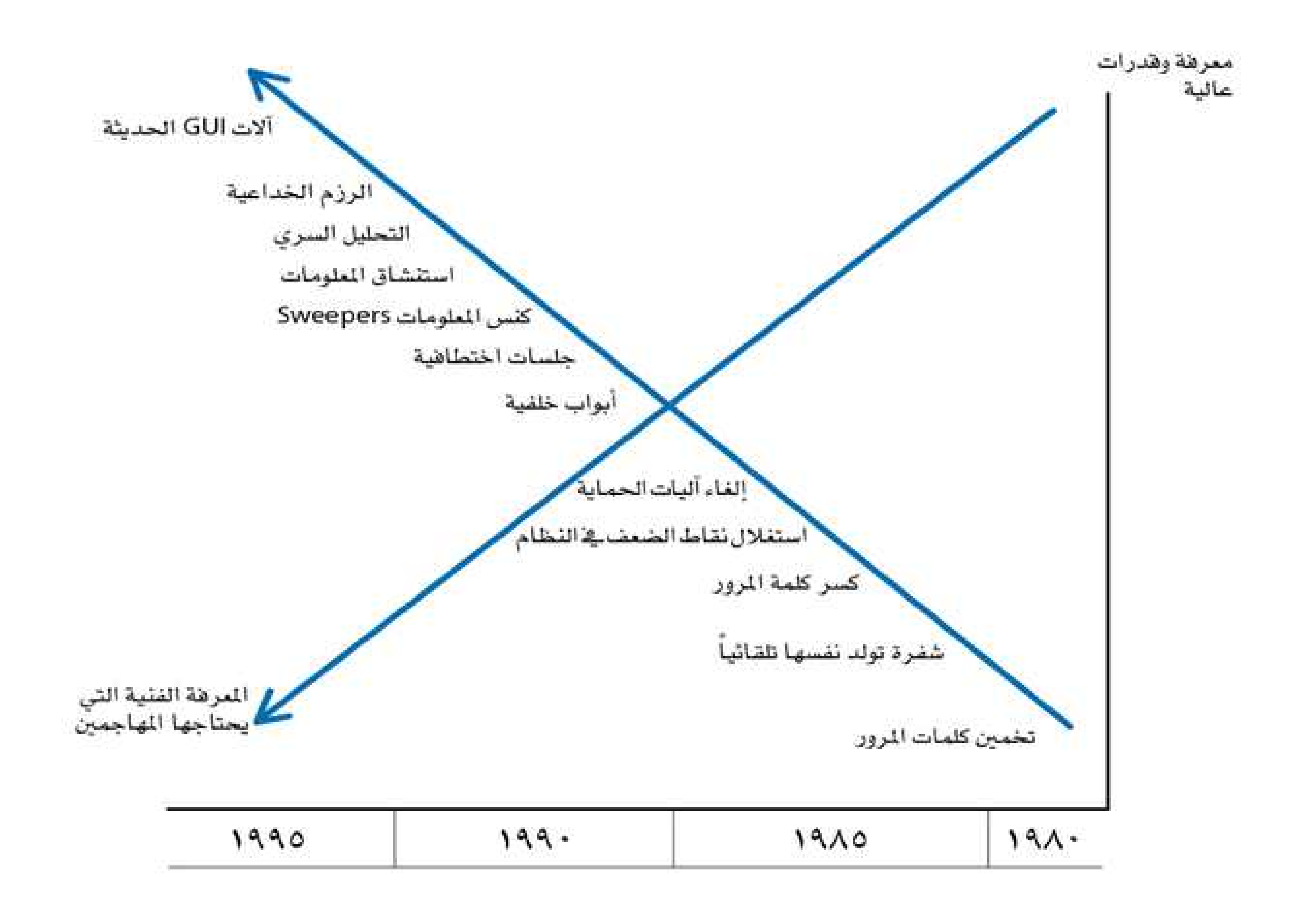
وقد حققت هذه الممارسات الجديدة، نجاحاً استثنائياً في مجالات متنوعة، مثل تطوير البرمجيات والتقارير البحثية والريادة والتميز في مجالات التصوير والأفلام، وكذلك الألعاب التي تمارس عن بعد. ويشير هذا إلى ظهور بيئة معلوماتية مكّنت الأفراد من القيام بأدوار وأنشطة حرة وغير ملزمة في اقتصاديات صناعة معلومات القرن الحادي والعشرين. وهذه الحرية الجديدة تشير إلى ظهور عصر واقعي عظيم، يمثل بعداً جديداً للحرية الفردية ومنبراً لتبادل الآراء ومشاركة ديمقراطية أفضل، وعامل مساعد لنشوء ثقافة ذاتية أكثر انتقاديه في اقتصاد عالمي يتزايد اعتماده على تقنية المعلومات، بصفتها آلية تحقق إصلاحات في النمو الإنساني في جميع أنحاء المعمورة.

ومع ذلك يبدو واضحاً أن الازدياد الكبير في المنتجات المعروضة في الأسواق الافتراضية، التي تديرها بيئة الإنترنت ويتحكم فيها الأفراد أو المؤسسات في مجال المعلومات والثقافة، بدأ يهدد صناعة الاقتصاد المعلوماتي التقليدي، ومع بداية القرن الواحد والعشرين بدأ العالم يكرس جهوده لتأسيس علم اجتماعي جديد لتنظيم البيئة الرقمية، فظهرت أعداد جمة من القوانين والأنظمة في مجالات شتى، مثل قوانين الاتصالات، وحفظ حقوق النشر، وتنظيم التجارة الدولية، ومعالجة أدق التفاصيل مثل قواعد تسجيل المواقع الإلكترونية، وتقنين حيازة المستقبلات التلفزيونية. وسيكون لنتائج هذه الجهود خلال العقود القليلة القادمة تأثير

مهم في وسائل المعرفة بالعالم، وإلى أي مدى وإلى أي شكل ستكون المجتمعات والأفراد، قادرين كأفراد مستقلين ومواطنين وشركاء في المجتمعات الثقافية أن يؤثروا في رؤية ما سيصير إليه هذا العالم في الحاضر والمستقبل.

رغم هذه الفوائد الواضحة، تتسبب الإنترنت في تهديدات ومخاطر حقيقية لقواعد البيانات ومراكز تخزين المعلومات[٩]، وخاصة الحساسة منها، بل إنها تمثل مصدر قلق لجميع قطاعات البنية التحتية، التي يتزايد اعتمادها على الإنترنت المترابطة عالمياً والمفتوحة للعموم، مما جعل الباب مشرعاً على مصراعيه أمام الإرهاب الدولي، وقراصنة المعلومات، فاضطرت الحكومات والمنظمات والمؤسسات بجميع فئاتها وأدوارها، لزيادة الاهتمام بالجانب الأمني لشبكات الاتصالات، وأماكن تخزين المعلومات، والحواسيب، لتجنب أعمال القراصنة والمخترقين، سواءً الأعمال التي تهدف لتغيير المحتوى أو سرقته أو تخريبه. ويعرَّف الاختراق أو الاقتحام بأنه محاولة الدخول غير المشروع أو إساءة استخدام نظام أو شبكة الحواسيب. وكلمة إساءة تأخذ معاني واسعة؛ فهي قد تعبر عن إساءة مؤلمة للغاية كسرقة بيانات سرية أو إساءة يسيرة، مثل الإزعاج عن طريق إغراق البريد الإلكتروني أو العبث به، باستخدام رسائل

شكل رقم(٣): تتناقص المعرفة المطلوبة لتنفيذ الهجوم مع تطور الأدوات المتوفرة للمهاجم



غير مفيدة بهدف تعطيل الموقع أو الدعاية، سواءً كان ذلك لأهداف سياسية أو شخصية، أو لمجرد اللهو وحب الاستطلاع.

إن محاولات الاختراق والوصول غير المشروع للمعلومات يتزايد بصورة مطردة مع نمو التقنية وحجم الشبكة وتزايد الاعتماد الرسمي عليها. كما أن كثيراً من المحاولات تكون بدقة عالية بحيث لا يترك المهاجم أي أثر يمكن أن يؤدي لاكتشافه. ولهذا قامت كثير من دول العالم بسن قوانين لتجريم القرصنة الإلكترونية، وفي الوقت نفسه تسعى شركات صناعة التقنيات الأمنية إلى تطوير وسائل حماية وجدران نارية، وهي برمجيات تستخدم كوسائل دفاعية لحماية الحواسيب والشبكات، وتمنع دخول المهاجمين للوصول لأجهزة الشبكة الداخلية بهدف حماية المعلومات، ومع كل ذلك؛ فإنه كلما طور العالم وسائل للحماية طور القراصنة والمهاجمون وسائل لكسرها وتلافيها، إما بتعلم طرق لكسرها أو استغلال خواص وثغرات جديدة في الشبكة لتجاوز الحماية (شكل ٣ المصدر: وزارة الدفاع الأمريكية، GAO/AIMD-٩٦-٨٤).

الفصل الثاني

التزايد المطرد في الاختراقات وأساليبها ومستوى خطورتها

الفصل الثاني

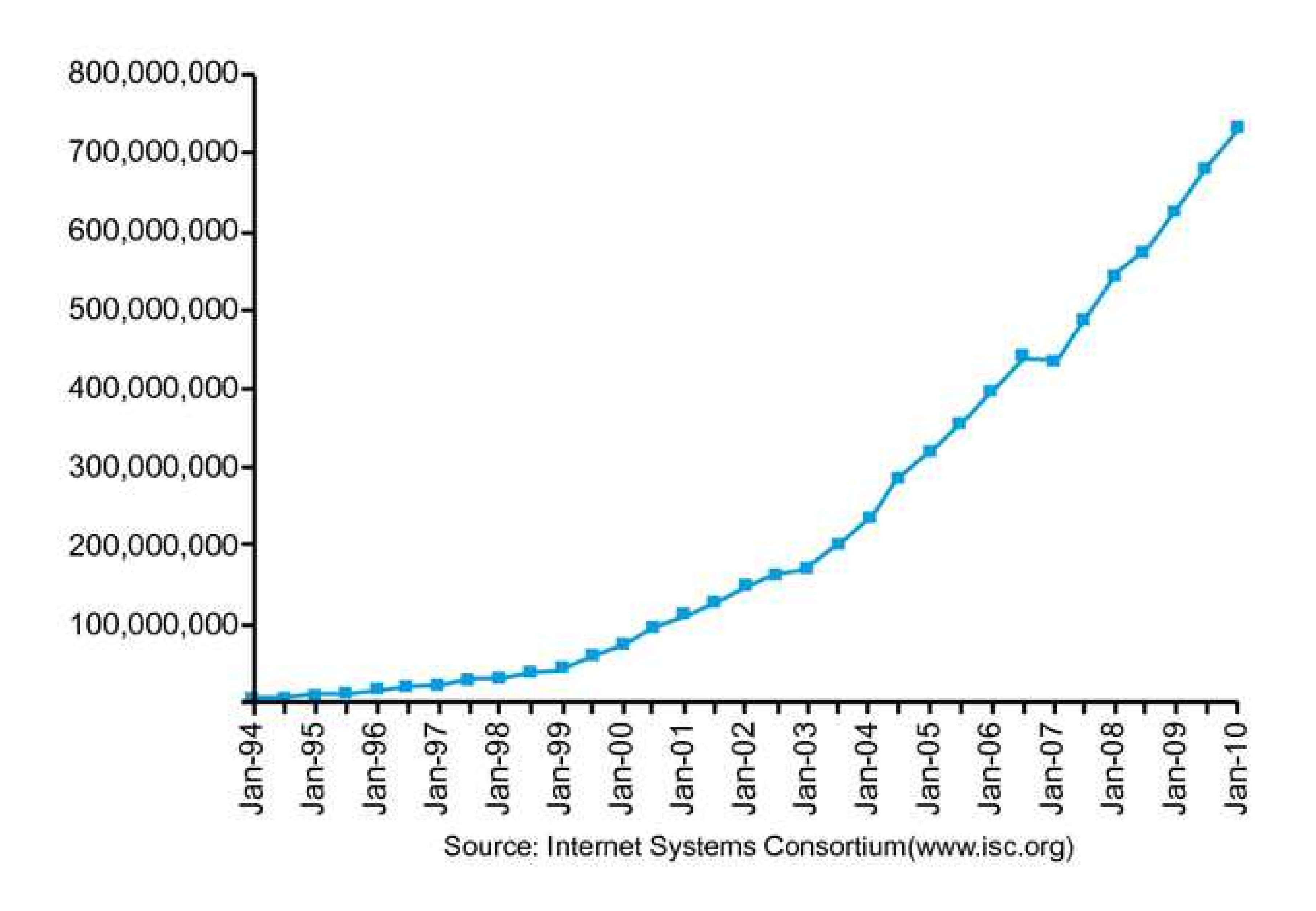
التزايد المطرد في الاختراقات وأساليبها ومستوى خطورتها

يقدر عدد الحواسيب المرتبطة بالإنترنت منذ عام ١٩٩٦م بحوالي ١٣ مليون حاسب، موزعة على ١٩٥ بلداً في جميع القارات، بما فيها قارة «أنتاركتيكا Antarctica» في أقصى جنوب الكرة الأرضية في القطب الجنوبي، وقد زادت الآن بكثير عن ذلك[١٠].

إنّ الإنترنت ليست نظاماً واحداً مستقلاً؛ بل تتكون كما سبق ذكره في الفصل الأول، من تجمع كبير لشبكات مترابطة بأسلوب غير محكم، يمكن التواصل معها عن طريق حواسيب شخصية مستضافة بطرق متعددة بما في ذلك الموانئ الإلكترونية Ports والموجهات Routers، والاتصال عن طريق الهاتف، والأقمار الصناعية، بمقدمي خدمة الإنترنت. ومن السهولة أن يتصل بالإنترنت أي شخص من أي مكان، إذا توافر له حاسب شخصي ثابت أو متحرك، عندما يكون في نطاق شبكة اتصالات ووسائل التوصيل المعروفة. كما يستطيع الأفراد والمنظمات الوصول إلى أي نقطة في شبكة الإنترنت، دون أي اعتبار للحدود الدولية والإقليمية وفي إي وقت على مدى الأربع وعشرين ساعة. ومن هذه السهولة المريحة للوصول إلى المعلومات، تأتي المخاطر الكبيرة، التي من بينها مخاطر فقدان معلومات مهمة أو تحريفها أو سرقتها أو إساءة استخدامها، مما يفسد الحاسوب الخاص بحفظها والتعامل معها.



شكل رقم: (٤) تعداد مواقع الإنترنت المستضافة من عام ١٩٩٠ إلى عام ٢٠١٠



Source: Internet Systems Consortium(www.isc.org)

وعندما تسجل المعلومات على هيئة رقمية وتحمَّل في حاسوب متصل بالشبكة؛ تصبح أكثر عرضة للعبث بها أو تحريفها، لأن المهاجمين لا يحتاجون دخول المكاتب أو المنازل، بل إنهم لا يحتاجون في أن يكونوا في الدولة نفسها أو المنطقة الجغرافية، فهم يستطيعون العبث بالمعلومات وسرقتها دون الحاجة إلى لمس ورقة أو تصويرها، لأنه يمكنهم نسخ صورة إلكترونية لكامل الملف، وتخزينه في حواسيبهم الشخصية، وإخفاء أي دليل على فعلتهم. ولا يتوقف الأمر عند هذا الحد، بل يتعداه كما سنرى في فصول لاحقة من هذا الكتاب، إلى تسهيل هجوم الإرهابيين وتمكنهم من جمع المعلومات والبيانات، التي يحتاجونها لتنفيذ خططهم الإرهابية الإجرامية.

عند ظهور الإنترنت، قبل خمسة وعشرين عاماً، كانت تتألف من أنظمة صغيرة من حيث العدد، وكان الارتباط بينها محصوراً آن ذاك في خطوط مستأجرة ذات نطاق ضيق وسرعات بطيئة، ولكنها سرعان ما نمت لتكوِّن ملايين الشبكات المنتشرة في جميع أنحاء العالم، وبهذا النمو السريع ظهر تزايد واضح، في عدم اتباع وسائل الأمن والحماية، وسوء الاستخدام من قبل معظم المستخدمين للأنظمة. ورغم إن تأمين وحماية أنظمة الحاسب أصبح الشغل

الشاغل للمهتمين بهذه الصناعة، حيث أوجدوا وفرة كبيرة من أدوات الأمن الإلكتروني، وعقدوا المؤتمرات، والحلقات الدراسية، والورش المتعلقة بذلك، وألفت الكتب، ووظف المستشارون المتمكنون، إلا أن أعداد الاختراقات في تزايد مطرد، والأدوات والتقنيات، التي يستخدمها القراصنة أصبحت أكثر تطوراً ودقة[١١]، وتأثيرهم أكثر انتشاراً وأهمية. وظهرت تبعاً لذلك أنواع كثيرة ومؤثرة من أصناف الهجوم في شبكة الإنترنت. لكن السؤال المطروح: ما هي أسباب ظهور هذه المخالفات؟ ولماذا يسعى أشخاص ومنظمات، بل وحتى حكومات لممارسة هذه الأعمال التخريبية؟ قد يكون للتوزيع الجغرافي للحواسيب والشبكات دور كبير؛ حيث كانت الأنظمة والشبكات منذ عقدين فقط، مملوكة وتشغل من قبل كيان منفرد، مثل الجامعات والشركات الكبيرة، وكانت معزولة في مباني آمنة محكمة، من حيث الوصول المادي والإلكتروني. أما في هذه الأيام؛ فإن الأنظمة مترابطة، ويمكن الاتصال بها من أي مكان في العالم، لأنها موزعة في جميع أصقاع المعمورة على هيئة حواسيب ثابتة ومحمولة، بعضها في المعامل، وأخرى في قاعات الاستقبال في الفنادق، وفي العربات والطائرات. ويمكن القول بثقة أن الشبكات العالمية ليس لها حدود أو نهايات، فالمستخدم في «آسيا» يستطيع الوصول إلى بيانات في أمريكا وأوروبا، والتعامل معها آنياً، ومن الصعب؛ بل من المستحيل السيطرة على التوزيع الجغرافي الذي سهل إمكانية الوصول وصعَّب التعرف على المستخدم ومدى شرعيته، وفيما لو أضطر العالم لتقييد الدخول وخفض إمكانية الوصول للمعلومات، بهدف خفض قدرة المهاجمين؛ فإن المكاسب المادية والثقافية والتعليمية، التي حققتها شبكات الإنترنت ستتأثر بشكل كبير. كما أن النمو الكبير في حجم وتعقيدات الشبكات صعّب سيطرة مدراء الأنظمة على شبكاتهم، حيث كان مدير النظام يستطيع فهم التقنية الأساسية لنظامه ويعرف مستخدميه، والسيطرة التامة على البرامج التطبيقية في نظام الحاسب المنفرد، أما اليوم فإن كل نظام يمكن أن يدعم عدداً كبيراً من المستخدمين الذين يشغِّلون برمجيات كثيرة مترابطة ومتوافقة مع بعضها رغم اختلاف مصادرها. كما أن مئات بل آلاف الحواسيب الشخصية يمكنها الارتباط بشبكات محلية تكوِّن فيما بينها آلاف الشبكات المحلية والشبكات العالمية عريضة النطاق. إن الفهم الجيد للأنظمة مثل فهم هيكليتها ونقاط مداخلها والسيطرة على العدد الكبير من مستخدميها والتطبيقات الكثيرة التي لا تعد ولا تحصى؛ كل ذلك يتعدى قدرات مدير النظام المنفرد، وهذا النقص في الفهم يؤدي إلى تقليص التحكم، ويسمح لتطور الثغرات الأمنية دون أن تلاحظ.

كما أن تواتر التغيير الناتج من نمو الحجم والتعقيدات في الأنظمة وتزايد سرعة التغيير في جوهر تغير التقنية والتطبيقات واستخدامات الحواسيب والشبكات، يجعل مدراء الأنظمة بعيدين كل البعد عن متابعة مهنتهم، فيما يتعلق بالبرمجيات والمعدات المستخدمة في الشبكات الكبيرة، والأنظمة، وقواعد المعلومات التي تخضع للزيادة والنقص بصورة مستمرة. فالتوصيل عن بعد للحواسيب في تغير منتظم، بحيث يستحيل على مدير منفرد متابعة هذه التغيرات المستمرة. وقد أضافت قابلية الحركة والانتقال، التي أحدثتها الحواسيب المنقولة والأجهزة اليدوية والاتصالات اللاسلكية والتقنية الخلوية، بعداً جديداً للتعقيدات والسيطرة على المدخلات للشبكات؛ ولهذا فإنه من الصعب التحقق من شخصية المستخدمين، إذا لم يكن ذلك مستحيلاً، وأصبحت متابعة الأنشطة المشبوهة في غاية الصعوبة. وجميع هذه القضايا مقرونة بطرق ووسائل أخرى، مثل الهندسة الاجتماعية، وهو اصطلاح جديد يطلق على الخدع التي يقوم بها بعض المخترقين عندما يوهم الشخص المتلقي بأنه مسؤول أو جهة رسمية ويطلب منه بعض المعلومات الخاصة، وسيتم شرح ذلك لاحقاً، وكذلك الاستفادة من العيوب الأمنية في البرمجيات مما يخلق بيئة يمكن أن ينشأ فيها ثغرات أمنية مؤثرة. وقد يكون من المدهش اعتبار وسائل أمن وحماية الشبكات غالباً ما يكون إجراءً غير أساسي أثناء تصميم الشبكة وتحديد تطبيقاتها ولا يلتفت إليه إلا بعد الانتهاء من التصاميم الأساسية وتنفيذها على أرض الواقع، مع أن إضافة الأمن الإلكتروني للشبكات القائمة في غاية الصعوبة وباهظ التكاليف، وجميع هذه الثغرات يمكن أن تستغل من قبل المهاجمين للوصول للبيانات والدخول للأنظمة بطرق غير شرعية.

ولدراسة الاختراقات فإن الباحثين يركزون في الغالب على حالات محلية ومخترقين محليين، أو على نظام تشغيل محدد، ومع أن دراساتهم توفر بعض الرؤى للقضايا الواجب فهمها، إلا أن الاختراقات يجب فهمها على المستوى الوطني والإقليمي والعالمي للشبكات العالمية المنتشرة هذه الأيام، وليس على المستوى المحلي في المنظمة أو الشركة أو الدولة.

ويمكن القول أنه ليس هناك حاسوباً أو شبكة حواسيب محمية بالكامل، فهناك ثغرات جديدة تكتشف وأخرى تستحدث على مدار الساعة[١٢]. والطريقة الوحيدة التي يمكن أن يتبعها المهنيون التقنيون والمهتمون بأمن الشبكات ليعودوا إلى بيوتهم وهم مطمئنون على شبكاتهم، أن يطبقوا قدراً كافياً من الوسائل والأدوات الأمنية، ويسعوا إلى تطبيق الأكثر في

اليوم التالي. وكل ما ينفق من جهد ومال لشراء أفضل أدوات الأمن المتوافرة، يصبح هباءً منثوراً، إذا لم يهتم العاملون على النظام بأخذ الحيطة والحذر وتأمين كلمات المرور الخاصة بهم، واختيار الأقوى منها، وقفل أجهزتهم عندما يغادرون أماكن عملهم. ولهذا فإنه يجب على المهنيين المتخصصين في أمن تقنية المعلومات توعية المستخدمين وتثقيفهم إلى أقصى ما يمكن، لضمان مراعاة أسس أمن تقنية المعلومات، حتى مع غياب الرقيب، والهدف هو جعل المستخدمين الأقل وعياً يفكرون في كل خطوة يخطونها ويتم تحفيزهم لجعل وسائل الأمن ضمن ممارساتهم اليومية. كما أن على جميع المعنيين بصناعة تقنية المعلومات وأمنها إعادة النظر في طرق ووسائل أمن البنية التحتية وحمايتها من التخريب والكوارث.

إن شبكات الإنترنت وشبكات الإنترانت تزدحم هذه الأيام بعدد كبير من المستخدمين والمتطفلين من جميع المستويات والفئات، الذين يحاولون التعرف على مستوى أمن الشبكات والأنظمة، بعضهم يهدف للاستيلاء على معلومات فكرية عالية، وآخرون يتصرفون بدوافع خبيثة، مثل الانتقام أو الاستحواذ على مكاسب الآخرين. ومهما كانت الدوافع؛ فإنه لا يوجد مخترق بريء أو مخترق حميد. كما أنه لا توجد وسيلة مضمونة يمكن أن تؤمن الأنظمة والشبكات. وأقصى ما يمكن أن يفعله المهنيون المتخصصون في تقنية المعلومات هو التأكد من قفل جميع الموانئ والبوابات الإلكترونية، وتشغيل جميع أدوات ووسائل الإنذار وتثقيف المستخدمين لمعرفة ما يجب البحث عنه.

تصنيفات المهاجمين

يُصنف المهاجمون للأنظمة الحاسوبية والشبكات إلى ثلاثة أصناف: «القراصنة التقنيون»، وهو تعبير يطلق على مستخدمي الحواسيب، الذين يحاولون الدخول إلى شبكات الاتصالات التابعة لمؤسسات كبيرة باستخدام حاسوب شخصي بهدف الحصول على معلومات سرية أو أموال بطريقة القرصنة الحاسوبية. و«هواة اختراق الحواسيب»، وهو تعبير يطلق على الشخص الخبير باستخدام وبرمجة الحاسوب، ويكون في المعتاد مولعاً بها ويتوق لمعرفة أسرارها التقنية وكيف تعمل، وهؤلاء يتمنون لو يطلق عليهم صفة «الهواة الحميدون»، أو «القراصنة الحميدون»، بدلاً من صفة قراصنة. بل يفضلون وصفهم بأنهم مهاجمون حميدون. والصنف الثالث «عيال النصوص Script Kiddies»، وهم في الغالب ليس لديهم معرفة أو إلمام بالتقنية

العميقة، ولكن يملكون مجموعة من الأدوات، التي أنتجها قراصنة متمكنون، ولديهم المعرفة الأساسية لاستخدامها لتنفيذ هجومهم.

وعلى أية حال؛ فإن المصطلح «مهاجم» يعني أي شخص يحاول الوصول إلى أنظمة الحوسبة دون أي حق مشروع. وبالإضافة إلى هذه التصنيفات؛ فإنه يمكن القول إن جميع التصنيفات الثلاثة، تنفذ من قبل فئتين: مهاجمون من الداخل؛ وهم المهاجمون المصرح لهم باستخدام النظام والوصول للشبكة، ويعدون مستخدمون شرعيون، ويشمل ذلك المستخدمين الذين يسيئون استخدام الصلاحيات، أو الذين يتقمصون شخصية من لهم صلاحيات أعلى منهم، وغالباً ما يكون الطمع هو الدافع الأساسي لهم، ومن ذلك أعمال النصب والاحتيال أو الانتقام، الذي يمارسه الموظف الساخط أو المفصول دون رغبته. أما المهاجمون من الخارج، فهم المهاجمون من خارج المنظمة أو الشبكة في محاولة لإفساد بيانات مزوِّد الشبكة وتغييرها، وإرسال رسائل دعائية متكررة ليس لها فائدة تسمى «سبام Spam»، كما أنهم قد يخترقون الجدران النارية. ويصل المهاجمون الخارجيون عن طريق الإنترنت أو الشبكة اللاسلكية أو خطوط الهاتف أو الاعتداء المادي، وهو الوصول الفعلي للأجهزة والعبث بمحتوياتها، أو عن طريق أنظمة وشبكات الشركات العاملة في النظام المستهدف المربوطين بالشبكة المعنية مثل شبكات المقاولين والمصنعين وغيرهم. وقد يكون هدفهم الكسب المادي، مثل سرقة بيانات البطاقات الائتمانية، أو تخريب نظام الشركة، أو القرصنة بهدف حرمان المجتمع مما ينشر في موقع محدد لأسباب سياسية، أو اجتماعية أو أخلاقية، أو أن يصدر من «عيال النصوص» وهو الشائع هذه الأيام لمهاجمة الأنظمة، باستخدام الثغرات الأمنية الموجودة أصلاً في النظام، ويضاف إلى كل هؤلاء المنظمات الإرهابية، التي تسعى للحصول على معلومات لاستخدامها في خطط أعضائها وأعمالهم الإجرامية.

وتشمل الطرق الأساسية التي يسلكها المهاجم، للوصول للنظام: الاختراق المادي، وهو عندما يكون المهاجم قادراً على الوصول الفعلي إلى الأجهزة المراد العبث بها، أي أنه يستطيع استخدام مفاتيح الإدخال في الحاسب، أو أنه قادر على تفكيك أجزاء الحاسوب مما يمكنه من الوصول إلى البيانات المخزنة في الحاسب. وتتدرج الأعمال التي يستحوذون عليها بهذه الطريقة من الحصول على صلاحيات تؤهلهم للعبث بالمحتويات، إلى إمكانية سرقة القرص الصلب وقراءته في جهاز آخر، وكذلك رفع مستوى صلاحيات المهاجم، وفي هذا

النوع من الهجوم يكون لدى المهاجم صلاحيات محدودة وله حساب في النظام، فإذا كان النظام غير محكم ويحتوي على ثغرات أمنية يمكن أن يستخدمها لرفع صلاحياته إلى مستوى أعلى. ومنها أيضاً الهجوم عن بعد، وهو يختص بالمهاجمين، الذين يحاولون الوصول للنظام من خارج المنظمة عن طريق الشبكة وليس لديهم أي صلاحيات عند بدايتهم، مع ملاحظة أن نظام كشف الاختراق عن بعد في الشبكة يهتم بالدرجة الأولى بالمهاجمين من خارج الشبكة، دون الالتفات إلى الوسائل الهجومية الأخرى.

تصنيفات أنواع الهجوم الشائعة

للهجوم ثلاثة تصنيفات:

أولاً: الاستكشاف Reconnaissance ـ وهذا النوع يشمل المسح بعدة طرق منها استخدام أداة «الطرق PING»، وهي عبارة عن أوامر تستخدم في الشبكات الحاسوبية، لمعرفة إمكانية الوصول لمزوِّد الشبكة المضيف من عدمه، ويكون ذالك بإرسال حزمة من الرموز إليه وقياس وقت انتقال الحزمة إلى المزوِّد المستهدف وعودتها إلى جهاز المرسل الموجود في موقع آخر قد يكون في نفس المكان أو في بلد آخر وتسجيل أي جزء يفقد من الحزمة. ومسح المداخل باستخدام أدوات مثل: نمط كتلة بيانات المستخدم User Datagram Protocol UDP: وهي وحدة تستخدم في تنظيم حركة نقل نمط كتلة بيانات المستخدم (UDP) وكل «كتلة بيانات واحدة» تحتوي على وحدة تراسل واحدة، كما أن الثمانية بايت الأولى فيها تحتوي على المعلومات العلوية Header Information، وبقية البيانات تحتوي على الرسالة، وهي من أقدم الأنماط المتوافرة منذ عام ١٩٨٠م، ويستخدم أيضاً نمط تراسل الإنترنت TCP أو نقل منطقة المجال Zone Transfer. ومن المحتمل أيضاً جدولة مزوِّد الشبكة العام لمعرفة ثغرات لغة CGI (common gateway interface)، وهي برامج صغيرة تنتهي بالامتداد CGI أو PL، وتتم كتابتها بلغة الأم Perl، ويصل حجم بعضها إلى ١كيلوبايت ولا تتعدى ٢٠٠ كيلوبايت. وأداة (CGI) عبارة عن وسيلة توصيل بين مزوِّد الشبكة والصفحة البيتية تسمح بتطبيق برنامج في الخلفية لتنفيذ مهمات لا يمكن إجراؤها، مثل تشغيل النماذج؛ وذلك لأن الصفحات البيتية لا يمكنها التعامل مباشرة مع القارئ، وكان ذلك مستحيلاً إلى أن ظهرت مشغلة نصوص جافا Java Script وغيرها من مشغلات النصوص، التي تمكنت من استخدام

واجهة البوابة العامة (CGI) لتوفير برنامج تفاعلي في الصفحة البيتية.

ثانياً: أسلوب الاستغلال العام، حيث يستغل المهاجمون جميع المعلومات التي حصلوا عليها مثل، المميزات المخفية، والخلول bugs، لضمان الدخول المتكرر للنظام.

ثالثاً: تعطيل الخدمة Denial of service (DoS)، وفي هذه الحالة يكون هدف المهاجم هو محاولة تعطيل النظام أو الخدمات، أو إغراق الشبكة، أو إغراق معالج البيانات CPU، أو تعبئة القرص الصلب؛ إذ أن المهاجم لا يبحث عن معلومات، ولكنه مجرد مخرب حاقد يعمل على منع الاستفادة من الأنظمة المستهدفة.

الهجوم باستخدام الثغرات الأمنية المحتملة وطرق استغلالها:

لا تخلو البرمجيات من الخلل، ولا يمكن لمدراء الأنظمة والمبرمجين تتبع وإلغاء جميع مكامن الخلل والثغرات الأمنية في النظام، وغاية ما يحتاج المهاجمون معرفته لا يزيد عن ثغرة واحدة للتسلل من خلالها. وكثيراً ما تستغل الثغرات في المزوِّد الحاسوبي Server المختص بالحماية أو التطبيقات البرمجية، التي يتعامل المستفيدون معها، أو نظام التشغيل أو الثغرات الموجودة في الشبكة نفسها. وعند اكتشاف ثغرات النظام يسعى المهاجم لاستغلالها، فالمهاجم المتمكن يستخدم وسائل وأدوات معقدة لاختراق النظام، أما المهاجم العادي فقد يستخدم الأدوات المجانية الشائعة، التي تعمل أوتوماتيكياً مثل Metasploit، وهو برنامج سهل الاستعمال يستخدم لتفحص الشبكة ومعرفة إمكانية الدخول إليها دون الحاجة للتسجيل، والهدف من طرحه مجاناً استخدامه في الفحوصات المشروعة لتحديد قوة الحماية في الشبكات، لكن القراصنة يستخدمونه لأغراضهم الخاصة. ويمكن استغلال عدد كبير من الثغرات، مثل ثغرات نصوص المزوِّد الجانبية Server-side scripts، التي تكون في الغالب غير آمنة، مثل واجهة البوابة العامة (CGI). وكذلك صفحات المزوِّد النشيطة Active Server Pages (ASP)، وهي عبارة عن تقنية تمكن المطورين من إنتاج صفحات تفاعلية ديناميكية. واستغلال إمكانية تمرير المدخلات غير السليمة للأمر «شل» Command Shell باستخدام أمر بادئة الرموز شل Meta-Characters Shell، حيث تستخدم متغيرات يمكنها تحديد اسم أي ملف في النظام وتستطيع كشف معلومات تتجاوز الحد المقبول. ومثل هؤلاء المهاجمين يمكن اكتشافهم من

خلال سجلات مزوِّد الشبكة server logs وبواسطة مراقبة حركة الشبكة عن طريق نظام كشف اختراقات الشبكة Network Intrusion Detection System (NIDS).

ويمكن أيضاً استغلال الهجوم على مزوِّد الشبكة Web Server Attack ـ نظراً لاحتمال وجود ثغرات أمنية، تتضح بعد تنفيذ نصوص المزوِّد الجانبية، وأكثرها شيوعاً طفح الذاكرة المؤقتة في حقول الطلبات التي ستشرح لاحقاً. ويمكن ـ أيضاً ـ القول أن جميع الحواسيب المستخدمة كمزوِّد للشبكة معرضة لمشاكل موجودة في تقنية الشبكات منذ القدم، مثل تعطيل المزوِّد بآلاف الشرطات (/) «Death by A Thousand Slashes». وقد سببت هذه المشكلة تحميلاً هائلاً لمعالج نظام «أباتشي Apache» عندما حاول معالجة كل صفحة دليل Directory، بسبب أن عنوان الموقع يحتوي على آلاف الشرطات (/)، ولا زال اكتشاف ثغرات أمنية جديدة في مزوِّد الشبكة مستمراً. وأفضل الطرق لحماية مزوِّد الشبكة هو متابعة الرزم الأمنية التي توزعها الشركة المنتجة لبيئة التشغيل، كما أن الهجوم على متصفح الشبكة Web Browser Attack يكون من خلال ثغرات أمنية موجودة أصلاً في جميع المتصفحات؛ فعنوان الموقع يمكن أن يتسبب في حالات إغراق الذاكرة المؤقتة، إما أثناء تحليل مقدمة روابط النصوص HTTP header، أو أثناء عرضها على الشاشة، أو أثناء معالجتها، مثل تخزينها في ذاكرة تخزين التاريخ المؤقتة Cache History كما يوجد عيب قديم في مستكشف الإنترنت يسمح للقراصنة وغيرهم بالتعامل معه، ويظهر عندما ينفذ المتصفح أوامر تنتهي بـ .LNK أو .URL وكذلك مشغل نصوص جافا Java Script، وهي الوسيلة المفضلة على الدوام عند القراصنة، بسبب أنها تستغل - في الغالب – وظيفة تحميل الملفات «File Upload» بأن تولد اسم ملف وتخفي بطريقة تلقائية زر الإرسال «SUBMIT». وقد تم إصلاح عدد كبير من هذه الأعطال؛ إلا أن القراصنة مستمرون في اختراع طرق جديدة لاحتواء تلك الإصلاحات.

أما الهجوم عبر نصوص الموقع المتقاطعة Cross-Site Scripting CSS، فهو يشمل توجيه المستخدمين لموقع تخريبي عن طريق «الارتباطات التشعيبية Hyperlinks» المصطنعة، لعلمهم أن المتصفحات التي بها ثغرات لا تتفحص هذه الأنواع من الروابط. ويمكن بعث معلومات كثيرة للموقع المستهدف، وهذا النوع من الهجوم يستخدم في الغالب في خطط الاصطياد Fishing، لأنه يخدع المستهدفين لزيارة مواقع عدائية. ويتوافر نموذج أمن قوي في

جافا Java؛ بيد أنه ثبت أن هذا النموذج يحتوي على بعض الأعطال، وإن كان يعد من أفضل العناصر الآمنة المتاحة، بالإضافة إلى أن قوة أمنها قد يكون بسبب عدم عملها، لكون تطبيقات جافا لا تحتوي على وسائل وصول للنظام المحلي، مع أنه أحياناً يكون من الأفضل لو كانت قادرة على الدخول للنظام المحلي، أي تطبيق نموذج الثقة الذي يمكن أن يهاجم بسهولة. كما أن تقنية ActiveX أكثر خطورة من جافا، لأنها تعمل من مضمون نموذج الثقة وتشغِّل رموزاً خاصة بها، ويمكن أن يؤدي هذا إلى التقاط فيروس قد يكون موضوعاً خطأً في برنامج شركة فرعية أو متعاونة.

ومن الوسائل المستخدمة تخمين رقم «متتالية نمط التحكم في الإرسال TCP»، وهو أن يستقل المهاجم ضرورة اختيار المستفيد لرقم تسلسلي عند بدء تشغيل رابط هذا النمط لتحديد النهاية الطرفية للمستخدم، وعلى ضوء ذلك يختار مزوِّد الشبكة رقماً آخر له، وفي الغالب يختار رقماً متسلسلاً يمكن تخمينه بسهولة؛ مما يسمح للمهاجمين من إيجاد موصل TCP من عناوين IP مزوَّرة، الأمر الذي يمكنهم من تحاشي وسائل الأمن. وهناك هجوم يعرف بتسمم نظام أسماء النطاقات (DNSP Domain Name System poisoning)، ويتم من خلال تخمين التسلسل، إذ إن مزوِّد نظام النطاقات يقرر أسماء النطاقات بصورة مكررة وعندما ينفذ طلب عميل، يصبح هو عميلاً للمزوِّد الذي يتلو ذلك في سلسلة المتتابعات، مما يسهل تخمين الأرقام المتتالية المستخدمة. وهذا يمكِّن أي مهاجم من إرسال طلب إلى مزوِّد أسماء نظام النطاقات DNS Server، وكذلك إرسال استجابة إلى «المزوِّد المزوَّر» لتبدو وكأنها من المزوِّد الذي يتلو في السلسلة، عندئذ سيثق في الاستجابة المزورة ويستخدمها مع عملاء آخرين في الشبكة. ويوجد عدد من المهاجمين الذين يستفيدون من القدرة على «تزوير أو خداع إجراءات الإنترنت المعيارية، IP spoofing»، فعندما يُرسَل عنوان المصدر مع كل حزمة من إجراءات الإنترنت المعيارية فإن ذلك لا يستخدم لأغراض التوجيه Routing، وهذا يعني أن المهاجمين يمكن أن يتقمصوا شخصية متصل حقيقي عند مخاطبة مزوِّد الشبكة، وفي هذه الحالة لا يستلم المهاجم أي استجابة رغم أن جهاز المتصل الفعلي يتلقى الاستجابات، ولكنه يهملها لأنها ليست ردوداً لمطالب صادرة من المتصل الحقيقي، وفي هذه الحالة لا يتلقى المهاجم أي بيانات بهذه الطريقة، ولكنه يتمكن من إجراء أوامر للمزوِّد المستهدف متظاهراً أنه المستخدم الفعلي، وهذه الوسيلة (IP spoofing) تستخدم كجزء من طرق منع أو تعطيل الخدمة في المواقع.

أساليب هجوم تعطيل الخدمة العامة Denial of Common Services:

استخدام طرقة الموت Ping-of-Death: في أواخر عام ١٩٩٦م ومع بدايات ١٩٩٧م انتشرت أخبار عيوب خطيرة في بعض تطبيقات الأنظمة التشغيلية في الشبكة العالمية، وتناقل القراصنة هذه الأخبار كطريقة لتعطيل الحواسيب ومزوِّدات الشبكة «Servers» عن بعد باستخدام الشبكة العالمية «الإنترنت»، وقد سمي هذا النوع من الهجوم «طرقة الموت»، وهي طريقة ميسرة التطبيق نسبياً، ولكنها خطيرة للغاية بسبب نسبة نجاحها العالية. ومن الناحية الفنية فإن هجوم «طرقة الموت» يتضمن إرسال حزمة إنترنت برتوكول أكبر من ٦٥,٥٣٥ بايت إلى الحاسوب المستهدف، ومع أن الحزم التي تتجاوز هذا الرقم غير مشروعة؛ إلا أن القراصنة يتبادلون تطبيقات وبرامج قادرة على تجاوز الرقم المشروع. ويمكن أن تكتشف الأنظمة التشغيلية المصممة بطريقة جيدة الحزم غير المشروعة، وتتعامل معها بأمان، لكن بعضها يفشل في ذلك. وقد أصبحت أداة نمط التحكم في رسائل الإنترنت ICMP اسم آخر للمشكلة لأنها غالباً ما تحتوي على حزمة كبيرة وتستطيع التعامل مع هذا الحجم من الحزم. بالإضافة إلى ذلك؛ فأن طبقة نمط التناقل الرئيسة المسماة «نمط كتلة بيانات المستخدم User Datagram Protocol UDP» تستطيع نقل «طرقة الموت»، وينطبق هذا الخطر على غيرها من الأنماط المعتمدة على نمط التراسل في الإنترنت، إذ أن كلها قادر على نقل «طرقة الموت». وما إن ظهرت هذه الطريقة من طرق الهجوم حتى بادرت كثير من الشركات المنتجة لأنظمة التشغيل في إنتاج تحديثات جديدة لتلافيها، وعمدت كثير من المواقع إلى استخدام جدران نارية لتلافي فقدان الخدمة بما في ذلك أساليب «طرقة الموت». وهناك تصنيفات كثيرة للثغرات الموجودة في البرامج وأنماط التراسل منها:

هجوم طفح الذاكرة المؤقتة Buffer overflow Attack:

يحدث طفح الذاكرة عندما يحاول برنامج أو معالج رقمي أن يخزن بيانات أكثر مما هو مسموح به في مستودع تخزين من مستودعات الذاكرة المؤقتة (The Buffer)، إذ إن مستودعات الذاكرة المؤقتة صممت لاستيعاب كمية محددة من البيانات، وهي البيانات أو المعلومات الإضافية التي تخزن فيها لحين تنتقل إلى وجهتها المقررة في البرنامج التطبيقي المراد تشغيله، إلا إنه عند تجاوز سعة المستودع فإن البيانات الزائدة تنتقل أو تطفح إلى مستودع

مجاور من مستودعات الذاكرة المؤقتة مما يتسبب في إفساد المعلومات الموجودة في المستودع المجاور، أو استبدالها بالمعلومات التي طفحت إليه. ورغم أن هذه الحالات كثيراً ما تحصل بمحض المصادفة بسبب أخطاء البرمجة الأساسية، إلا أنها تمثل نوع شائع من أنواع الهجوم الإلكتروني يعرف بـ«هجوم طفح الذاكرة». وفي حالة الهجوم يتعمد المهاجم إضافة رموز مصممة لتنشيط إجراء أو أوامر محددة، وهي عبارة عن أوامر للحاسوب المستهدف لتخريب بعض الملفات أو تغيير المعلومات أو الإطلاع على معلومات سرية، ويحدث طفح الذاكرة المؤقتة نتيجة للإطار، الذي توفره «لغة سي C language» والممارسات الضعيفة أثناء البرمجة. وجميع المشاكل التي تنشر غالباً ما تكون بسبب هذه المشكلة، ومن أمثلة ذلك تخصيص ٢٥٦ رمزاً لحفظ اسم المستخدم بواسطة المبرمج الأساسي. فعندما يحاول المهاجم إدخال اسم مستخدم غير حقيقي، بحيث يكون أطول مما هو مخصص له؛ فقد تظهر الثغرة الأمنية، وكل ما يحتاج المهاجم فعله هو إرسال ٣٠٠ رمز بما فيها الرمز الذي سيطفح للمستودع المجاور، حيث يستجيب المزوِّد الحاسوبي للأمر عند تلقيه الرمز الذي وضعه المهاجم.

ويمكن للمهاجمين معرفة هذا الخلل بعدة طرق: منها الحصول على البرنامج المصدر «Source Code» من شبكة الإنترنت، حيث أن المهاجمين يبحثون بانتظام عن الثغرات الموجودة في البرمجيات المنشور مصادرها الترميزية، وتحتوي على ثغرات من هذا النوع، ويمكن للمهاجمين كذلك تفحص البرنامج بأنفسهم لمعرفة وجود مثل هذه الثغرات، كما أنه يمكنهم - أيضاً - تتبع كامل مداخل النظام ومحاولة إغراقها ببيانات عشوائية، فإذا فشل النظام يشير ذلك إلى احتمال عالي للوصول من خلال مدخل يتم اختياره بعناية.

الهجوم باستخدام العيوب في تهيئة النظام System Configuration Bugs:

عيوب التهيئة الافتراضية Default Configurations:

تصل معظم الأنظمة للمستفيد النهائي بتهيئة افتراضية ضمن تعليمات تنصيب البرامج التطبيقية بهدف تسهيل التنصيب والاستخدام، ولسوء الحظ فإن سهولة الاستخدام تعني سهولة الاختراق، ولذلك فقد تنبه مصممو البرامج والأنظمة في السنوات الأخيرة لهذه المشكلة وشرعوا في إصدار أنظمة ذات قدرات أمنية أفضل، محاولين تلافي التعليمات التي قد

تؤدي إلى فتح بعض الثغرات والموانئ التي يمكن أن يستغلها المهاجمون، ومع ذلك فلا تزال هناك مخاطر مرتبطة بالتهيئة الافتراضية.

تشغيل خدمات غير ضرورية Running Unnecessary Services:

يمكن من حيث المبدأ تهيئة جميع البرامج لتعمل دون مراعاة لمتطلبات الأمن الإلكتروني، وأحياناً؛ قد يفتح مدراء النظام بوابة في مداخل النظام بدون قصد، رغم أن جميع تعليمات التشغيل تنص بشدة على ضرورة قفل كل وظيفة أو بوابة ليس لها حاجة ضرورية وأساسية في الجهاز أو النظام لضمان عدم إحداث ثغرات عرضية غير متوقعة. علماً أن شركات مراجعة أمن الشبكات والأنظمة تبحث عن هذه الثغرات، وتشعر مدراء الأنظمة عنها.

العلاقات المؤتمنة بين الأنظمة Trusted Relationships:

تتكون جميع الأنظمة المترابطة من عدد من الحواسيب الثابتة والمتنقلة، والأجهزة البينية، وشبكات الاتصال. وتعرَّف جميع هذه المعدات لمزوِّد الشبكة المختص بالحماية ووسائل الدفاع، وتصبح التعاملات فيما بينها علاقات موثوقة، بحيث تمرر المعلومات منها وإليها حسب الحاجة. ولأن قوة الشبكة هي قوة أضعف مكوناتها، فإن المهاجمين يعتمدون كثيراً على استغلال العلاقات بين الأنظمة المختلفة، ويسعون لمعرفة المكونات الأقل أمناً في الأنظمة المترابطة.

الهجوم باستخدام عيوب التصميم Design Flaws:

لا تخلو البرامج من العيوب الناتجة بسبب أخطاء فنية في التصاميم الأساسية، وحتى عندما يكون تنصيب البرنامج صحيحاً ومتماشياً مع التصميم؛ فإنه كثيراً ما يُكتشف ثغرات في أصل التصميم تمكن المهاجمين من الوصول مثل:

عيوب نمط التحكم في الإرسال والإنترنت TCP /IP Flaws:

صممت الإجراءات المعيارية للإنترنت قبل أن يكون هناك تجارب مع الهجوم الواسع

والمتسارع، الذي يلاحظ اليوم في الشبكة، ونتيجة لذلك فقد ظهرت عيوب تصميمية متعددة قادت إلى احتمال وجود مشاكل أمنية، مثل «هجوم سميرف SMURF» الذي أخذ اسمه من اسم البرنامج الذي ينفذ الهجوم، وهو عبارة عن طريقة تمكن المهاجم من إرسال كمية محدودة من الحركة المرورية الإلكترونية، التي تتسبب في إحداث تضخم في الحركة المرورية على صورة انفجار تفاعلي يتضخم في الموقع المستهدف يؤدي إلى إغراقه وتعطيله، ويكون ذلك كما يلي:

يستخدم المهاجم أداة «الطرق Ping» بإرسال حزمة من الرموز إليه وقياس وقت انتقال الحزمة إلي المزوِّد المستهدَف وعودتها إلى جهاز المرسل الموجود في موقع آخر قد يكون في المكان نفسه أو في بلد آخر، وتسجيل أي جزء يفقد من الحزمة. وتعمل هذه الخاصية بأن ترسل طلب الحصول على صدى (Echo) من حزمة نمط التحكم في رسائل الإنترنت (ICMP) Internet Control Message Protocol للمزوِّد المستهدف وتنتظر استجابته، وذلك بعد أن يقوم المهاجم بتزوير عنوان برتوكول المصدر Source IP Address فيظهر بصفة عنوان الموقع المستهدف، ثم يستخدم أسلوب بث عناوين التراسل الموجهة Directed Broadcast Addresses، أي أنه يبعث حزمة نمط التحكم في رسائل الإنترنت عن طريق الموجِّه Router المتصل بالشبكة المحلية إلى عناوين البث لشبكات خارجية قد تقع في منطقة جغرافية بعيدة، فتلتقط جميع المضيفات Hosts العاملة في الشبكة المحلية نسخة من صدى الحزمة المعاد بثها كما هو مفترض، وترسل إجابة للطلب لما تعتقد أنه المصدر (أي للمصدر المزوَّر)، وفي حالة وجود عدد كبير من الأجهزة المضيفة العاملة (في الغالب يزيد عن ١٠٠ جهاز)؛ فإن نسبة التضخيم ستكون هائلة. وينبغي ملاحظة أن المهاجم يستخدم في الغالب حزمة كبيرة تكون في حجم أكبر حزمة يمكن أن تتعامل معها تقنية نمط الإيثرنت، وهو البرتوكول المستخدم عادة لتوصيل الحواسيب بالموجهات Routers بهدف زيادة مستوى التأثير. وكلما زادت سرعة شبكة اتصال المهاجم كان الضرر على الموقع المستهدف والشبكة المرتبط بها أكبر، ولا يقتصر الضرر على الجهاز المضيف المستهدف، باستخدام هذا الأسلوب، بل إن إغراق الحركة سيكون هائلاً جداً لدرجة أنه يتسبب في تأثيرات سلبية خطيرة على اتجاه الحركة المعاكس الآتي من الشبكة أو الشبكات المستهدَفة، وهكذا ستتأذى المنظمات المستهدَفة، بسبب أن الشبكات التي تضخمت حركة تراسلها، ستتأثر هي الأخرى بحيث تصبح مستنقعاً لصدى حزمة الاستجابة كما أراد لها المهاجم.

ولتوضيح ذلك، فإنه ـ وعلى سبيل المثال ـ يمكن أن تصور خمسمائة جهاز توجِّه هجوماً قوياً ومتتالياً على مزوِّد شبكة معين مثل «اليوتيوب»، بحيث يكون الهجوم على كل ما في الموقع من روابط للتحميل مثل صورة لعبة برنامج أغنية، أو مقطع فلم على رسائل الموقع الشائع استخدامه عند الشباب والشابات، وتفعيل زر مثل «اضغط هنا» واستمتع بأجمل وأحلى مواضيع هذا المزوِّد، عندئذ لن يتمكن المزوِّد المستهدَف من الرد على كل اتصال موجه له في الوقت نفسه بهذا القدر العالي من الحجم والسرعة. مما يؤدي غالبا ـ عند استخدام توقيت وتخطيط مناسب ـ إلى عزل الموقع تقريبا عن بقية الشبكة .

ممارسة إدارة سيئة للنظام:

كثيراً ما يتكاسل مدراء الأنظمة عن وضع كلمة مرور خاصة بهم، إما إهمالاً أو بسبب الاستعجال وضيق الوقت عند تهيئة النظام ووضعه في الخدمة، ولسوء الحظ فإنهم لا يجدون وقتاً إضافياً لكتابة كلمة مرور فيما بعد، مما يسمح للمهاجمين وخاصة المهاجمين من الداخل، للدخول بسهولة، والعبث بالنظام. وأول ما يقوم به المهاجم تفحص شامل للأنظمة وتحديد الأنظمة، التي لا تحتوي على أي كلمة مرور لمدير النظام أو إنها تحتوي على كلمة مرور شائعة مثل أسماء الأقارب، أو تواريخ الميلاد ونحو ذلك.

الهجوم عن طريق كسر كلمة المرور:

ليس هناك شك أن كلمة المرور هي أضعف حلقة مستقلة في السلسلة الأمنية؛ لأنه من السهل كسرها، لذا لا يمكن الاعتماد عليها كعامل حماية منفردة للتعريف بهوية المستخدم، مما يتطلب حماية الأنظمة، التي تحتاج للحماية بوسائل متعددة من أنظمة الحماية، مثل Smart Crack و Token وأنظمة السمات الحيوية Biometrics أو الشهادات الرقمية، رغم أن تطبيق نظام متعدد الوسائل قد يكون صعباً وباهظ التكاليف، وبعض الأنظمة قد لا تكون مهيأة لدعم مثل هذه الأنظمة الوقائية، لذلك فإنه من الضروري معرفة الطرق المختلفة لكسر وتخمين كلمات المرور والعمل على مقاومتها: مثل استنباط كلمات المرور ميسرة التخمين كاستخدام اسم الشخص أو اسم أحد أطفاله أو أحد أقاربه أو موديل سيارته، وهناك من يستخدم كلمة «مدير Admin»

أو يترك حقل الكلمة خالياً. وفي الغالب يحاول المهاجمون على الدوام التعرف على هذا المزيج من كلمات المرور المحتملة قبل الانتقال إلى أي طريقة أخرى للحصول على كلمة المرور. وهناك الهجوم باستخدام القاموس وهو أن يستخدم المهاجمون برامج تحاول كل كلمة في القاموس، ويتم ذلك إما بالدخول المتكرر للنظام أو عن طريق تجميع كلمات مرور مشفرة ويحاول الحصول على ما يطابقها بتشفير مشابه لكلمات القاموس، ويحتفظ المهاجمون بقواميس بلغات مختلفة لهذا الغرض، وجميعهم يستخدمون قواعد معلومات شبيهة بالقواميس مثل الأسماء، وقوائم تحتوي على كلمات المرور الشائعة. وهناك الهجوم القهري Brute Force Attacks، وهو يشبه الهجوم باستخدام القواميس، إذ يحاول المهاجم استخدام جميع توليفات الرموز والحروف والأرقام باستخدام معالج حديث CPU، ويمكن اكتشاف كلمة من أربعة حروف في دقائق معدودة، بينما يستغرق كسر الكلمة المكونة من ثمانية رموز من الحروف الكبيرة والصغيرة والأرقام ورموز التوقف، عدة ساعات أو أكثر، إلا أنه يمكن اختصار الوقت إلى حد كبير باستخدام عدد من الحواسيب لتعمل على المشكلة نفسها في الوقت ذاته، وهو ما يعرف بأسلوب توزيع المهمات.

وهناك نوع آخر من الهجوم وهو استخدام القوائم المجهزة مسبقاً Pre-Computed Tables، وتسمى أحياناً «قوائم قوس قزح»، وفي الغالب تكون القوائم مجهزة باستخدام عدة حواسيب وبمجرد توليد مثل هذه القوائم فإن وقت محاولة الكسر لأي كلمة مهما كانت قوتها يكون قصيراً لدرجة كبيرة، وحتى الكلمات المعقدة يمكن معرفتها بسرعة فائقة وخلال دقائق فقط. وهناك أدوات شائعة مثل Rainbow Crack, Ophcrack and Cain & Abel تستخدم القوائم المجهزة، كما أن القوائم نفسها متوافرة في الإنترنت، ويوجد مواقع يمكن أن تكسر كلمات المرور بسعر معقول أو تبيع القوائم المجهزة. وخلاصة القول، أن كلمات المرور في الحقيقة لا تعد وسيلة حماية مجدية ضد إصرار المهاجمين، بل أنه من الضروري تطبيق طرق حماية أخرى.

الهجوم عن طريق سرقة كلمات المرور:

اصطياد النصوص الواضحة:

بعض الإجراءات المعيارية مثل (Telnet, FTP, HTTP Basic) تستخدم كلمات مرور غير مشفرة عند الانتقال بين الجهاز العميل ومزوِّد الشبكة عن طريق الأسلاك، إذ يستخدم

المهاجم محلل إشارات الإجراءات ومراقبة الأسلاك بحثاً عن كلمات المرور وبمجرد اكتشافها يتم استخدامها للدخول للنظام.

اصطياد النصوص المشفرة:

معظم الإجراءات المعيارية تشفر كلمات مرور بطريقة من طرق التشفير، وفي هذه الحالة يضطر المهاجم إلى تنفيذ هجوم بالقواميس أو هجوم قهري على كلمات المرور لمحاولة تجاوز التشفير، مع ملاحظة أن النظام لازال يجهل وجود المهاجم، لأنه خامل تماماً ولم يبعث أي شيء إلى النظام، فالاستحواذ على كلمات المرور لا يتطلب إرسال أية معلومات، لأن جهاز المهاجم يستخدم لاستنباط كلمة المرور فقط.

إعادة إرسال كلمة المرور المشفرة:

في بعض الحالات لا يحتاج المهاجم إلى فك تشفير كلمة المرور، ولكنه يسجل الكلمة المشفرة كما هي ويستخدمها للدخول إلى النظام. وهذا يتطلب في العادة برمجة خاصة لاستخدام كلمة مشفرة.

سرقة ملف كلمات المرور:

تخزن قاعدة المعلومات الخاصة بالمستخدم بكاملها في ملف منفرد في القرص الصلب. ففي «يونيكس تخزن في الملف / etc/passwd» وفي ويندوز تخزن في ملف يسمى SAM file، أو ملف قاعدة البيانات النشطة Active directory database مثل ntd.dit، وفي أي من الحالتين فبمجرد أن يحصل المهاجم على هذه الملفات؛ فإنه يمكنه تنفيذ برامج الكسر لمعرفة الكلمات الضعيفة الموجودة في الملف.

التفتيش المباشر:

إحدى المشاكل التقليدية في أمن كلمات المرور هو اختيار كلمة طويلة ومن الصعب تخمينها بهدف تصعيبها على الهجوم القهري والهجوم باستخدام القواميس، لكن مثل هذه الكلمات يصعب تذكرها، لذلك يلجأ الكثير من الناس إلى كتابتها في مكان أعمالهم ومكاتبهم. لهذا فإن معظم المهاجمين يفتشون مقرات عمل الأهداف على أمل الحصول على قصاصة بها

كلمة المرور وكثيراً ما تكون تحت مفاتيح الإدخال، وجميعهم يتدربون على اختلاس كلمات المرور أثناء طباعتها بملاحظة حركات المستفيد أو المستخدم بالنظر من خلفه.

الهندسة الاجتماعية:

هناك استراتيجية شائعة وناجحة وهي ببساطة، الاتصال بعامل مقسم المساعدة الفنية helpdesk وإخباره أنه المستخدم «س» وأنه مدير قسم تقنية المعلومات في الشركة وأن لديه إيجاز مهم يريد تقديمه للمدير العام، ولكنه غير قادر على الدخول للمزوِّد «ص» ليسترجع ملحوظاته، ويرغب في تغيير كلمة المرور ليتمكن من الدخول، لأنه ليس لديه سوى دقيقتين. والملاحظ أن كثيراً من الفنيين يُخدعون بمثل هذا الادعاء. لذا تعمل معظم الشركات لاتباع سياسات وإجراءات مشددة وتوجه فنييها إلى عدم إعطاء أو تغيير كلمات المرور، حتى ولو طلب منهم مدراؤهم ذلك، ومع هذا كثيراً ما تنجح هذه الخدعة. وهناك وسيلة أخرى تعرف بالتصيد، وتقع خطة «التصيد» في هذا النوع من أنواع الهجوم وتشمل ظهور المهاجم بهيئة المصدر الموثوق، مثل البنوك وشركات التأمين ونحو ذلك. وفي الغالب فإنه يتم ذلك عن طريق البريد الإلكتروني لخداع المرسل إليهم للإفصاح عن معلومات سرية، مثل كلمات المرور ومعلومات بطاقات الائتمان. ويسمى هذا الأسلوب أحياناً «أسلوب رسائل الاصطياد الإلكتروني»، وهو عبارة عن إرسال كم هائل من الرسائل الإلكترونية إلى أكبر عدد من الناس، كما حصل في عام ٢٠٠٥م عندما انتحل شخص ما صفة بنك سعودي وأرسل رسالة إلكترونية لعدد من المواطنين والمقيمين كان محتواها كما يلي:

«عميلنا العزيز، ... يود قسم الأمان في البنك لدينا أن يخبرك بأنه تم اتخاذ بعض الإجراءات للارتقاء بمستوى الأمان في تعاملاتك البنكية عبر الإنترنت، وذلك لمواجهة المحاولات المستمرة لاختراق الحسابات البنكية بصورة غير قانونية. للوصول إلى النسخة الأكثر أماناً من منطقة العملاء، يرجى اجتياز عملية الترخيص.... بالنقر هنا للانتقال إلى صفحة الترخيص ... نود أن نحيطكم علماً بضرورة التعامل مع إجراءات الأمان الجديدة بصورة جدية للغاية والاطلاع عليها الآن ... مع أطيب الأمنيات، ... قسم الأمان».

وبعد النقر على الرابط المرفق مع الرسالة يتم الانتقال للموقع المحتال الذي يبدو بشكله موقع البنك الأصلي، الموقع يطلب المعلومات الاعتيادية للدخول، وهي اسم المستخدم وكلمة

المرور ورقم الهوية، وبعد الإدخال يتم الانتقال مباشرة لصفحة البنك الرئيسة بعد ما حصل المحتال على المعلومات الكافية للوصول لحسابك في ذلك البنك، العنوان المزيف تم تسجيله في اليوم السابق للهجوم فقط في تايوان ثم أُنشئ موقع مشابه تماماً لموقع البنك السعودي، وكان هدف المحتال هو الحصول على أسماء مستخدمين وكلمات مرور لبعض الضحايا، التي قد يستفيد من استخدامها للوصول لحساباتهم وتحويل مبالغ منها للخارج.

استحصال الحروف عند إدخالها من لوح المفاتيح:

يتم هذا الهجوم بتسجيل ضربات إدخال الحروف من لوح المفاتيح، إما عن طريق تخزينها في ملف باستخدام برامج خاصة يتم تنزيلها وتخزينها في النظام المستهدَف، أو بوضع جهاز صغير بين لوح المفاتيح والحاسوب، وبهذا يتمكن المهاجم من جمع كمية كبيرة من المعلومات من بينها كلمات المرور. ومن الواضح أن توصيل جهاز بالحاسوب قد يكون صعباً ومعرضاً للكشف ويتطلب وصولاً فعلياً للموقع والحاسوب، وغالباً ما تستخدمه المنظمات الاستخباراتية. والشائع من هذه الأساليب هو تسجيل إلكتروني لضربات المفاتيح، أو وضع حاوية بها عدد من: cash memory USB في مدخل مبنى المكاتب المراد مهاجمتها أو إهداؤها للضحية، أو توزيعها في المؤتمرات، فبمجرد توصيلها بالحاسوب يتم إنزال «حصان طروادة Trojan Horse»، وحصان طروادة عبارة عن شفرة صغيرة يتم تحميلها لبرنامج رئيسي من البرامج الشائعة التي يكثر استخدامها، ويقوم ببعض المهمات الخفية، غالبا ما تتركز على إضعاف قوى الدفاع لدى الضحية أو تقويضها ليسهل اختراق جهازه وسرقة بياناته، وسمي بهذا الاسم لتشابه عمله مع أسطورة حصان طروادة الخشبي، الذي اختبأ بداخله عدد من الجنود اليونانيون، وكانوا سبباً في دخول القلعة وفتح مدينة طروادة.

أمثلة لمراحل الاختراقات النمطية:

مرحلة طريقة الاستطلاع

وفي هذه المرحلة يسعى المهاجم لجمع أكبر قدر من المعلومات دون كشف نفسه، ويفعل ذلك بالحصول على معلومات عامة، أو الظهور كمستخدم عادي، وفي هذه الحالة يصعب الشعور بوجوده، لأنه يبحث في قاعدة بيانات عامة مثل: «من يكون www.who.is»، وهي

قاعدة بيانات مجانية تحتوي على معلومات مُلاك المواقع والصفحات البيتية في الإنترنت، ويمكن من خلالها الحصول على اسم مالك أو ملاك الموقع وأرقام هواتفهم، وبالنظر في مكان تسجيل الموقع المستهدف يمكن معرفة أكبر قدر من المعلومات عن المالك للموقع وعن الشبكة والأشخاص المعنيين فيها، كما أن المهاجم يمكنه التنقل في قوائم مزوِّد أسماء نظام النطاقات Domain Name System Server (DNS) الخاصة بالموقع المستهدف، وذلك باستخدام أدوات مثل «nslookup, dig» أو أي أدوات أخرى من التي تستخدم لنقل منطقة النطاق Domain Zone Transfers، لمعرفة اسم المزوِّد أو الحاسوب المستخدم، كما أن المهاجم يمكنه تصفح مواقع عامة أخرى مثل موقع الإنترنت العام، الخاص بالشخص المستهدف ومواقع الـFTP العامة «The Public Web Sites and Anonymous FTP Sites». كما أنه قد يبحث في مقالات إخبارية وتصريحات صحفية عن الشركة المستهدفة.

مرحلة المسح الإلكتروني

يستخدم المهاجم تقنية اقتحامية لتفحص المعلومات دون التسبب في أي ضرر، فيتصفح جميع صفحات الموقع المستهدف بحثاً عن ثغرات في واجهة البوابة العامة Common Gateway Interface (CGI)، وقد ينفذ بحث عن طريق أمر «الطرق» ping (انظر ملحق ٢) ليتعرف على الأجهزة العاملة في الشبكة المستهدفة، وقد يستخدم المهاجم أدوات، مثل Nessus، وهي أداة موجودة في شبكة الإنترنت وتوزع بالمجان، ليكتشف محتويات الشبكة وما يتوافر فيها من ثغرات. وبهذا فإن ما قام به المهاجم لا يعد فعلاً غير عادي في الشبكة، كما أنه لم يقم بأي اختراق، وإلى هذا الحد يكون أقصى ما يمكن أن يعرفه المدير الأمني عن طريق برامج وأدوات كشف اختراقات الشبكة، أن هناك من يتفحص مقابض الأبواب، ولكن ليس هناك من حاول فتح الباب حتى الآن.

مرحلة استغلال المعلومات المجَمَّعة

تبدأ هذه المرحلة بتجاوز المهاجم الخطوط الأمامية، والبدء في استغلال الثغرات الأمنية للجهاز المستهدَف، وقد يستخدم المهاجم المتمرس طُرقاً معقدة كأن يستغل تلك الثغرات عن بُعد، حين أن المهاجمين الأقل خبرة «عيال النصوص» مثلاً، قد يستخدمون أدوات أوتوماتيكية مثل «Metasploit»، التي لا تحتاج سوى معرفة يسيرة، مثل القدرة على استخدام متصفح

إنترنت وعنوان نمط الإنترنت IP Addresses للنظام المستهدف للتَّمكن من استغلال النظام.

إيجاد موضع قدم

في هذه المرحلة يكون المهاجم قد أنشأ موضع قدم لنفسه في النظام باختراقه، وهدفه الرئيس الآن هو إخفاء جميع الدلائل، التي تشير إلى الهجوم ومعالجة ملفات التتبع والتسجيل لضمان عودته للنظام متى ما شاء. وقد يثبتّ شيءً من أدوات الهجوم مثل «Rootkits»، لتمكنه من معاودة الدخول وإخفاء تحركاته واستبدال بعض الخدمات المتوفرة بعدد من «أحصنة طروادة»، التي تحتوي على مداخل خلفية لكلمات المرور أو ينشئ حسابات خاصة به. والمشرف الأمني الجيد يستطيع في الغالب اكتشاف المهاجم في هذه المرحلة بملاحظة ملفات النظام المتغيرة؛ إلا أن المهاجم المتمكن يستطيع تغطية تحركاته لتلافي الاكتشاف حيث يستخدم النظام كوسيلة للعبور إلى نظام آخر، لأن معظم الشبكات لا تستعمل سوى دفاعات قليلة ضد الهجوم الداخلي.

مرحلة العمل من أجل الربح

هذه هي المرحلة الأخيرة، و فيها يبدأ المهاجم بالاستفادة من موضعه في النظام المعتدى عليه ليسرق البيانات السرية والخاصة، والإساءة في استخدام موارد النظام كأن يهاجم مواقع أخرى من الموقع الذي تم استغلاله، أو تشويه صفحات الموقع وإفسادها.

أدوات المسح الاستطلاعي العام

يوجد أدوات كثيرة للمسح والاستطلاع منها أداة Nessus، وهي إحدى أدوات المسح المجانية الشائعة، التي تتوافر بهدف مساعدة مدراء التشغيل لاكتشاف الثغرات الأمنية وقفلها، لكن قراصنة الحواسيب يستفيدون منها لأغراضهم المشبوهة. وتعمل هذه الأدوات المجانية في بيئات مختلفة مثل «بيئة لينكس، وبيئة ويندوز»، وهي تجمع معلومات كثيرة لمعرفة وتحديد الأنظمة عن بعد وكشف ما فيها من ثغرات أمنية أو فجوات يمكن التسلل من خلالها. وينفذ المسح بطرق متعددة أكثرها شيوعاً الفحص عن طريق أداة الطرق Ping Sweeps، التي

تحاول الوصول إلى الشبكة بإرسال رموز عدد من عناوين نمط الإنترنت IP addresses لمعرفة الأجهزة المتصلة بالشبكة باستخدام تلك العناوين. ومعظم أجهزة المسح المتطورة تستخدم إجراءات «أنماط» متنوعة، منها نمط إدارة الشبكات الميسرة The SNMP protocol، الذي ظهر في أواخر عام ١٩٨٠م بسبب الحاجة لإدارة النمو المتزايد في شبكات الإنترنت والتأكد من توافر خدمات معينة فيها، ونمط التحكم في الإرسال الـTCP، ويستخدم المهاجمون هذه الأنماط للبحث عن بوابة أنماط التحكم في الإرسال، التي تكون في الغالب مفتوحة لأغراض صيانة النظام ويستغلونها لتنفيذ اختراقاتهم.

ومن الصعب اكتشاف هذه الأنواع من الماسحات، لأنها إجراءات خالية من التوصيلات Connectionless، وطريقة عملها إرسال حزم عشوائية للمدخل المستهدف ومعظم الأجهزة تستجيب برسالة ICMP التي تفيد أن «المُدخِل المقصود غير موجود». ويعني ذلك عدم وجود خدمات تستمع لذلك المُدخِل؛ إلا أنه بمجرد اكتشاف هذا الخطأ تم إصلاحه في كثير من الأنظمة بعدم الاستجابة لرسائل الـICMP، لهذا فإنه لا يمكن استخدامها في جميع الحالات. وبالمثل يكون التعامل مع الهجوم بالتعرف على نظام التشغيل OS system، فبمجرد إرسال حزمة ICMP غير مشروعه أو غريبة أو TCP packets يتمكن المهاجم من التعرف على نظام التشغيل، لأنها تعمل بمقاييس استجابة ثابتة ومعروفة لتحديد استجابة الجهاز للحزم المشروعة، وتكون الاستجابات خاصة بكل نظام تشغيلي مما يجعله منتظم في استجابته لأي مُدخَلات قياسية، ولا تستجيب للمُدخَلات غير المشروعة أو الخاطئة وبعبارة أن كل نظام تشغيل له بصمة معيارية يمكن للمهاجم التعرف عليها لتحديد نوع الآلة أو الجهاز، وهذا النوع من النشاط يتم في مستوى منخفض Low Level، مثل الماسحات المختلسة التي لا يسجل النظام دخولها وخروجها.

الفصل الثالث

البرمجيات المجانية المفتوحة المصادر ومساهمتها في التطور التقني لإرهاب الدولي والقرصنة الإلكترونية

الفصل الثالث

البرمجيات المجانية المفتوحة المصادر ومساهمتها في التطور التقني للإرهاب الدولي والقرصنة الإلكترونية

يستفيد الإرهاب العالمي إلى حد كبير من كل ما يتوافر في شبكات الإنترنت، ومن بينها البرامج المجانية المفتوحة المصدر «Open Source Code»(١٣) التي تعد من أهم مخرجات ظاهرة الإنترنت، وهي محصلة الإنتاج التعاوني العالمي المبني على الموارد العامة ويتميز باللاملكية واللامركزية. ولم يكن هذا الأمر ممكناً لولا توافر الإنترنت بهذا المستوى، وانتشارها على كامل الرقعة الجغرافية العالمية. ولم يتصور أي شخص في الماضي أن البرمجيات المفتوحة ستصل إلى ما يمكن اعتباره ثورة حقيقية في هذا المجال، وأن يتعاون ملايين البشر في شتى أنحاء العالم لحل ما يواجه أي مستخدم لأي برنامج تطبيقي لأي أداة أو آلة دون تمييز، سواءً كان المستخدم جماعة، أو دولة، أو منظمة إرهابية، أو كان فرداً أو كان عالماً أو باحثاً يسعى لخدمة البشرية أو طالباً في جامعته.

فعلى سبيل المثال؛ لو أراد مستخدم في قرية من قرى أدغال أفريقيا أو الهند أو أفغانستان أو أمريكا أو أوروبا ـ مع افتراض أنه يمتلك الحاسوب والطابعة المناسبة وأنه متصل بالشبكة العالمية وأنه يريد أداة تطبيقية تمكنه من طباعة صورة بالألوان ـ معرفة التركيب الكيميائي لأي مادة متفجرة أو كيف يخترق الحواسيب الحكومية، وطلب المساعدة للحصول على برنامج

أو معلومات تمكنه من ذلك؛ فإنه سيفاجأ بالردود السريعة من شتى أنحاء العالم تشرح له كيف يفعل ذلك. أما إذا كان لديه القدرة على البرمجة، ولو بمستوى متواضع؛ فإنه يستطيع أن يحصل على مصادر الترميز Source Code لبرنامج كتبه شخص ما ونشره في الشبكة وسمح لأي شخص بتعديله وإضافة الوظائف غير المضمنة وإعادته للشبكة بنفس الرخصة الأساسية للكاتب الأصلي.

وقد انتشرت ظاهرة البرامج المجانية المفتوحة المصدر بسرعة هالة، وتبع ذلك نمو سوق افتراضية تعتمد على المتاجرة عن طريق الإنترنت، ومبنية على مبدأ التعاون الجماعي واللاملكية. وقد اتضح للصناعة في شتى المجالات، بما في ذلك صناعة الإرهاب والدمار، أهمية وقوة البرمجيات المجانية «المفتوحة المصدر»، وبادرت كبرى الشركات بالاستفادة من هذا المصدر التقني المجاني، وسخرته لجني الأرباح، ودخلت شركات كثيرة في هذا المجال واستفادت منه ومن أوائلها شركة آي بي إم IBM، التي تبنت تطوير البرنامج التشغيلي المجاني الشهير «جينو/ لينكس» ليتلاءم مع احتياجاتها، ثم أعادته للشبكة بنفس ترخيص كاتبه الأساسي وتفاصيل كاملة عن «مصادر الترميز Source Code» الخاصة به التي قامت بتطويرها وسمحت لمن أراد استخدامها. و(جينو/ لِينُكس بالإنجليزية: GNU/Linux)؛ ويسمّى أحيانًا لينكس، هو نظام تشغيل مجاني مفتوح المصدر، وهو جزء من مشروع جينو، ويخضع لدرجة عالية من الحرية في تعديل وتشغيل وتوزيع وتطوير أجزائه، ويصنف ضمن عائلة «يونكس Unix»، إلى جانب أنظمة أخرى بعضها مملوك وبعضها متاح للعموم. وسرعان ما تلقفت الجهات الحكومية العالمية، مثل وزارة الدفاع الأمريكية، وكذلك كبرى الشركات، مثل شركة HP وغيرها برنامج «جينو/ لِينُكس»، واعتمدت عليه بعد تطويره كبرنامج تطبيقي لشبكاتها، وبهذا نشأت وسيلة نمت بتسارع مذهل للتعاون العالمي تهدف إلى تطوير البرمجيات المبنية على جهود مشتركة.

ويعتمد هذا البرنامج على مساهمات جمة يقدمها عدد كبير من أشخاص يسعون لتحقيق مشروع مشترك ضمن حوافز متنوعة، ويشتركون بمساهماتهم دون أن يفرض أي منهم حقوقاً لمنع أي مشارك من استخدام المساهمات أو المنتج النهائي، وذلك لتلافي تملك أي شخص أو فئة معينة من المشاركين للمنتج. ويحتفظ المشاركون بحقوق النسخ لمساهماتهم، ولكن عليهم ترخيصها لأي شخص في نموذج تراخيص شامل يسمح باستخدام المواد بقيود تجعل من

المستحيل لأي جهة أو شخص منفرداً أو طرفاً ثالثاً أن يمتلك المشروع. ويعد هذا النموذج من التراخيص من أهم المبتكرات التشريعية، ويسمى «ترخيص العموم لحركة البرمجيات الحرة General Public License-GPL»[١٤]، وهو النموذج الأساس لما تلاه من التراخيص، التي تحقق الغرض نفسه. وتعد البرامج المجانية المفتوحة من أهم الخدمات، التي تقدمها الإنترنت كعنصر من عناصر البنية التحتية، وبما أن الهدف منها هو خدمة المجتمع بأكمله وبجميع فئاته ومكوناته وتوفير المعرفة للجميع؛ فإنها مثل أي مكون من مكونات البنية التحتية لا يمكن فتحها للعموم، كما لا يمكن في ذات الوقت قفلها عن قوى الشر والإرهاب الدولي!

وقد انتشرت ظاهرة البرمجيات المفتوحة بشكل ملموس في مجتمعات الشبكات والتقنية في العالم، حيث أصبحت حدثاً واضحاً في ثورة الإنترنت معتمدةً على الانتشار الواسع لشبكات الاتصال ونقل المعلومات في كل مكان، مع إمكانية الوصول إليها في أي وقت، وأدى هذا الانتشار إلى تحول جذري في نطاق الإنتاج الجماعي ومقياسه ونجاعته لكامل نظام إنتاج المعلومات والثقافة، واستفاد منها كامل المجتمع المدني التقني بشقيه المهتمين بحماية المعلومات والشبكات ومجتمع القرصنة والإرهاب. وكلما انخفضت أسعار الحواسيب وزادت سرعة نقل المعلومات وأصبحت متوافرة في أي مكان وزمان بأسعار منخفضة، زادت ظاهرة البرمجيات المجانية «مفتوحة مصدر الترميز» إلى أن تحول العالم بأسره إلى مركز أبحاث وتطوير وقواعد معلومات مفتوحة لكل من يرغب في البحث والتطوير أو الاستفادة من نتائج بحوث الآخرين.

وهكذا دخل الإرهابيون والقراصنة في هذا المعمل الضخم. فظهرت مواقع يديرها ويحررها مجموعات كبيرة من قراصنة الحواسيب وإرهابيي الشبكات والمتعاطفين مع المنظمات الإرهابية، ونشروا الأدوات التي تساعدهم على اختراق الشبكات وقدموا تجاربهم لكل من يريدها بالاستراتيجية نفسها، التي استخدمها علماء ومهنيو التقنية. كما توافرت كثير من المواقع التي تسعى لحل المشاكل والصعاب التي تواجه مخترقي شبكات الحواسيب، بما في ذلك مواقع تقدم قوائم جاهزة تستخدم لكسر كلمات المرور المفتوحة والمشفرة ونشر وتوزيع الثغرات الأمنية في الأنظمة، وتوضيح طرق وأساليب الوصول للأنظمة عن طريق تلك الثغرات. كما ظهرت مواقع تشرح طرق وأساليب التفجير وصناعة القنابل المدمرة وطرق الإخفاء والتفخيخ وأساليب اختراق الحلقات الأمنية ومواقع لتجنيد العاطلين وصغار السن

للانخراط في المنظمات الجهادية الانتحارية ومواقع تنشر الرعب والخوف في المجتمعات الإنسانية. كما استغلت تلك المجموعات الشبكة العالمية لأغراضها الإعلامية.

والسؤال المطروح: لماذا؟ وما هي الدوافع التي تحفز القراصنة والإرهابيين الإلكترونيين لمواصلة الاختراقات وتطويرها؟ ونشرها؟ وللإجابة عن هذه التساؤلات يقول القرصان الشهير «إريك ستيفن ريموند» في مقابلة أجراها معه «أندرو ليونارد»[١٥]: «إنني مثل معظم قراصنة الإنترنت لا يهمني في الحقيقة الكسب المادي. إنني أفعل ما أفعله في الدرجة الأولى للرضا عن مستوى مهاراتي الفنية والحرفية، وكل ما أريده هو أن أعرف أن ينظروا إلى ما قدّم على أنه فن جيد، فالإنسان لا يعرف أنه يتطور في الاتجاه الصحيح، إلا إذا أكدت الحقائق والناس الآخرون له ذلك. لهذا فإن معظم حوافزي الأساسية، كما هو الحال لدى معظم القراصنة، هي السعي إلى أن يعتقد القراصنة الآخرون أنني مؤثر ومنتج ومصمم جيد وما إلى ذلك». كما يقدم «إريك ريموند» موضوعاً شيقاً بعنوان «كيف تصبح قرصاناً؟»، يوضح فلسفة القراصنة، نشره في موقعه[١٦].

وللفائدة، فقد تم وضع بعض المواقع التي تسرد مواقع القراصنة وصفحاتهم البيتية ومصادر متعلقة بالقرصنة، وهي مواقع مأمونة (انظر ملحق ١)، وفيما يتعلق بمواقع القرصنة؛ فإن على القراء اتخاذ الحذر والحيطة إذا أرادوا تصفحها لأن بعض المواقع المشهورة يديرها قراصنة ومنظمات قرصنة محترفة، ويُنصح بعدم زيارتها، وعلى من يريد تصفحها أن يتحمل مسؤولية ذلك، وعليه اتخاذ الإجراءات التي تؤمن بياناته ومعلوماته وبرامجه لأن القراصنة يتركون بعض البرامج المؤذية والفيروسات في الحواسيب الخاصة بمواقعهم.

ويشاهد اليوم ظاهرة إنتاج جماعي للمعلومات بمقياس واسع وإمكانية التعامل مع مهام أكثر تعقيداً مما كان ممكناً في الماضي في مجال الإنتاج الجماعي، سواءً في مجتمعات تطوير التقنية لخدمة المجتمعات أو تطوير وسائل وأدوات الاختراقات لخدمة القراصنة والإرهاب.

الإرهاب والإعلام وتقنية الشبكات المفتوحة

استغل أعضاء المنظمات الإرهابية الدولية، التسهيلات الكثيرة والتطور التقني في انفتاح الشبكات وسهولة الوصول إليها والبرمجيات المفتوحة المصادر والمجانية، وأصبحوا يعمدون

إلى التسلح بوسائل الإعلام المختلفة لتسويق أغراضهم وغاياتهم، وتوظيفها في تضليل الأجهزة الأمنية واكتساب السيطرة على الرأي العام، عن طريق نشر أخبار العمليات الإرهابية التي يقومون بتنفيذها، على اعتبار أن الحملات الإعلامية التي تغطي هذه العمليات تساعد على تحقيق واستكمال أهدافهم. وفي ندوة استضافها الكونغرس الأميركي في يوليو ٢٠٠٧ عن مخاطر مواقع التنظيمات الإرهابية على الإنترنت باللغة العربية ولغات أخرى في الترويج لعملياتها، يقول «يغال كارمون» رئيس معهد أبحاث الشرق الأوسط في واشنطن[١٧]: «إن كثيراً من الشركات الغربية، بما فيها الأميركية، تقدم خدمة الإنترنت للجماعات الإرهابية بأسعار زهيدة، دون وعي لأخطار تلك المواقع على الأمن القومي الأميركي». وأوضح «كارمون» أن هناك مواقع تتمتع بحضور في شبكات الإنترنت، وهي متعاطفة مع الإرهاب الدولي، وتستغل مبادئ حرية التعبير للترويج للإرهاب ونشر ثقافة تدريب العناصر الإرهابية على صنع القنابل والمتفجرات. وعلى وجه الخصوص، فإن القاعدة تروج لعملياتها عن طريق مؤسسات إعلامية خاصة بها مثل، مؤسستي «السحاب» و«الفرقان»، وهما مثال للمؤسسات المتخصصة في خدمة الإرهاب الإعلامي العالمي.

وتحاول الحكومات العربية منع جميع أنواع التطرف والإعلام الإرهابي حالما تكتشفه، ولكن الشركات الأميركية تجد صعوبة في اكتشاف المواقع، التي تخدم الإرهاب بسبب صعوبة معرفة أهدافها ومحتوياتها والقائمين عليها، حيث إن المنظمات الإرهابية تنشر أهدافها تحت أغطية متنوعة ليس من السهل كشفها. ومن الواضح أن الغرب يتعامل مع المحتويات الإعلامية من منطلق حرية التعبير، ولكن القاعدة تنظر للإعلام كوسيلة للتخطيط والاتصال والتمويل والتدريب والإرهاب. ورغم أن الشركات الغربية، وعلى وجه الخصوص الموجودة في الولايات المتحدة الأمريكية مثل جوجل Google وياهوو Yahoo وميكروسوفت Microsoft، في غنى عن المردود المالي المحدود الذي يقدمه الإرهابيون؛ إلا أن معظم الشركات تقدم لهم خدمات مجانية. وتطالب الجهات الأمنية بفرض عقوبات على الشركات التي تستضيف المواقع المشبوهة؛ لكن مثل هذا الإجراء غير عملي، فالشركات الكبرى والمعروفة لا تتعمد تقديم أي خدمات للإرهاب مهما صغرت هذه الخدمات، لكنها تحتاج إلى آلية لإبلاغها عن محتويات أي موقع له علاقة بالإرهاب أو القرصنة، وقد لا يكون هناك حاجة لاستخدام وسائل قانونية، وتشريعية، يمكن من خلالها منع الشركات من استضافة

مواقع قد تروِّج للإرهاب، إذا ما تم إيجاد آلية لإبلاغ الشركات المزوِّدة لخدمة الإنترنت بمحتويات المواقع الإرهابية قبل السماح بها.

والمتصفح العادي يستطيع تمييز المواقع المتعاطفة مع الإرهاب، وكذلك الشخصيات الإلكترونية الوهمية لأعضاء منظمة القاعدة، مثل شخصية أبو دجانة الخراساني ـ الإلكترونية الذي يعد المسؤول الأول عن الهجوم الذي وقع في قاعدة «تشابمان» العسكرية الأمريكية السرية بولاية خوست جنوب شرق أفغانستان يوم الأربعاء ٣٠-١٢-٢٠٠٩م، وهي قاعدة تستخدم كمركز عمليات واستطلاع متقدم لوكالة المخابرات المركزية الأمريكية، وتستخدم لتوجيه طائرات بدون طيار لمهاجمة حركة طالبان والقاعدة في المنطقة الحدودية المجاورة لمناطق القبائل الباكستانية، الذي سقط فيه سبعة ضباط من الاستخبارات المركزية الأميركية مع النقيب «الشريف علي بن زيد آل عون»، الذي أقيمت له مراسم عزاء في الديوان الملكي، فيما لم تؤكّد الرواية الرسمية الأردنية ما جاء في رواية «طالبان» وفي التسريبات الأميركية بأن النقيب الأردني قد سقط في ذلك التفجير نفسه.

وأبو دجانة كان طبيباً يحمل الجنسية الأردنية، يدعى «همام خليل أبو ملال البلوي». وكان يستخدم اسماً مستعاراً هو (أبو دجانة)، وهو ناشط بالمنتديات الجهادية الإرهابية. وقال الحاج «يعقوب» ـ وهو مسؤول بطالبان ـ في تصريحات له: «إن المخابرات الأردنية كانت قد تصورت أنها جندت أبو دجانة ليقابل «أيمن الظواهري» الرجل الثاني في تنظيم القاعدة، ويزودهم بمعلومات عن طالبان في وزيرستان، غير أنه تمكن من تضليل المخابرات الأردنية والأمريكية على مدار عام كامل. وأوضح الحاج يعقوب: «كنا نمد المخابرات الأردنية ـ عن طريق أبو دجانة - بمعلومات مضللة عن الحركة لكسب ثقتها، وكانوا يمررون تلك المعلومات إلى المخابرات الأمريكية، واستمرت اللعبة طوال عام كامل، حتى قرر عملاء المخابرات المركزية نقل همام إلى خوست للحديث معه عن تفاصيل بعض الأهداف والمعلومات، فانتهز الفرصة للقيام بهجومه»، ونظراً للثقة التي بناها همام مع المخابرات الأردنية، التي لديها مقر كامل في خوست، وكذلك مع المخابرات الأمريكية عن طريق المخابرات الأردنية؛ فإنه لم يتعرض للتفتيش، ونقل إلى مقر القاعدة، التي نفذ فيها الهجوم فقام بتفجير نفسه، وقتل وجرح عناصر من «سي آي إيه».

واعتبرت العملية أكبر خسارة في صفوف المخابرات الأمريكية خلال الـ ٣٠ عاما الماضية، وذلك بعد مقتل ٨ من عملائها في تفجير السفارة الأمريكية ببيروت عام ١٩٨٣م، حسب ما تناقلته الصحف والمنتديات العالمية والعربية خلال ذلك التاريخ، أي ٣٠/ ١٢/ ٢٠٠٩م.

وهكذا يظهر بوضوح استغلال الإرهاب للإنترنت ووسائل الإعلام عن طريق الوسائل المتاحة له وأهمها تقنية شبكات الاتصالات ونقل المعلومات لترويج الأفكار الإرهابية ودعمها، من خلال المحاولات المستمرة في البحث عن الدعاية الإعلامية لتسليط الضوء على وجوده وأغراضه. وتشير كثير من الأبحاث النفسية، أن الإرهابيين قد لا ينفذون عملياتهم إذا علموا مسبقاً أنها لن تحظى باهتمام إعلامي، لكشف حجم الخسائر التي ألحقوها بأعدائهم، على اعتبار أن الحرب النفسية تعمل عملها فقط عندما تجد من يهتم بها. وفي هذا الإطار وصفت «مارجريت تاتشر» رئيسة الوزراء البريطانية السابقة هذه الدعاية (المجانية) بالأكسجين اللازم للإرهاب، الذي لا يستطيع الاستغناء عنه[١٨].

ولا يخفى على أحد أن تغطية الحدث الإرهابي إعلامياً تحقق مكاسب تكتيكية واستراتيجيه لمنفذيه، وأن علاقة الإرهاب بالإعلام ظاهرة أشبه ما تكون بعلاقة بين طرفين، أحدهما يصنع الحدث والآخر يقوم بتسويقه. وهذا الأمر يطرح أسئلة عديدة ربما تفيد الإجابة عنها في تشخيص هذه العلاقة، ومعرفة الظروف والأجواء العامة المسؤولة عن انتشار ظاهرة الإرهاب. ومن البديهي طرح أسئلة مهمة، مثل: ما مدى إمكانية أن يعيش الإرهاب بدون إعلام؟ وعن مدى تغذية التغطية الإعلامية للأعمال الإرهابية؟ وما مدى تشجيع الإعلام للأشخاص الذين يقفون وراء الإرهاب، لارتكاب المزيد من هذه الأعمال الإجرامية؟ وهل يساعد الإعلام على نشر الثقافة الإرهابية، ومن ثم الإسهام في زيادة معدل ظواهر العنف والإرهاب؟ هذه كلها تساؤلات مشروعة ومهمة، وتحتاج إلى التمعن والإجابة.

وتعمل المنظمات الإرهابية على عدة محاور باستخدام تقنية شبكات المعلومات أولها: إنشاء مواقع بأسماء مختلفة وأهداف غير معلنة لتجنيد الأعضاء في جميع أنحاء العالم، مستغلين حرية الرأي والتعبير، التي تكفلها الدساتير والقوانين الدولية وحرية الإعلام، ومتخذين من مبادئ حقوق التعبير مبررات لتفسير اتجاهاتهم. والمحور الثاني، هو إرهاب المجتمعات المستهدفة بنشر صور الإرهاب لإظهار جبروتهم وعدم إنسانيتهم بهدف التخويف وبث

الرعب. ويساعدهم في ذلك، بقصد وأحياناً دون قصد؛ الإعلام بجميع وسائله التي يستخدمها الإرهابيون من خلال بث الفزع والخوف بين الناس عن طريق بعض القنوات الفضائية والإذاعات والصحف والمجلات والمواقع الإلكترونية ببث الخطابات التكفيرية، وتبني سياسة نشر العنف والفوضى والسعي لإثارة الفتن وتزييف الحقائق، وعرض الأفلام والمقاطع، التي تصور عمليات الذبح وحز الرقاب. أما المحور الثالث؛ فهو محور إعلامي يعوضهم عن عدم قدرتهم على إنشاء وسائل إعلام تقليدي نظراً لمحاربة العالم لهم وعدم تمكنهم من إنشاء محطات تلفزيونية مرخصة، وبدلاً من ذلك يضعون أشرطة مصورة وتقارير في مواقع يعلمون سلفاً أنها ستحجب، ويخبرون عنها بوسائل مختلفة مثل الاتصال بالقنوات الرسمية وإعطائهم الرابط الذي يحتوي على الشريط الذي يريدون بثه.

وضوح العلاقة بين الإرهاب والإعلام والحكومات، ولكن!!

يدرك الإرهابيون والحكومات ووسائل الإعلام علاقة الإعلام ومسؤوليته عند تغطيتها للحوادث الإرهابية ولكن من وجهات نظر متباينة، فالإعلام يوجه ردود الفعل أثناء الحوادث الإرهابية، وغالباً ما يوفر مكاسب تكتيكية واستراتيجية للإرهابيين وأهدافهم الشمولية. والتحدي الذي يواجه الحكومات ووسائل الإعلام، هو فهم ديناميكية المشروع الإرهابي، وتطوير سياسات لخدمة مصالح المجتمع والحكومات والإعلام. ولا ينكر أحد أن الإعلام قوه فاعلة للمواجهة بين الإرهاب والحكومات لأن تأثيره في الرأي العام لا ينحصر فقط، في تفاعل الحكومات مع الحدث؛ بل يتعداه إلى ردود فعل المجموعة، التي نفذت العملية الإرهابية. وينظر الإرهابيون إلى التغطية الإعلامية على أنها مقياس مهم في نجاح عملياتهم، وتظهر خطورتها الإعلامية أثناء عملية اختطاف الرهائن، إذ إن الأخبار الإعلامية هي الوسيلة الوحيدة أمام المختطفين لمعرفة سلسلة الإجراءات التي يتبعها فريق تخليص الرهائن، مما قد يتسبب في تعقيد مهمة الإنقاذ.

وبالمستوى نفسه تستخدم الحكومات الإعلام لحشد الرأي العام الدولي ضد الدولة أو المجاميع، التي تستخدم التكتيك الإرهابي. وبعبارة أخرى؛ فإن الإرهاب يسعى لتحقيق دعاية مجانية، لأن المنظمات الإرهابية غير قادرة على امتلاك وسائل إعلامية تقليدية. لذا فهم يبحثون عن أي تغطية إعلامية لعملياتهم الإرهابية، التي تظهر للعالم وجهات نظرهم وتأكيد أن

قضيتهم لا يمكن تجاهلها ولا بد من مناقشتها. ويرى الإرهابيون أن المقابلات مع زعمائهم، وخاصة المقابلات غير المنقحة، تعد مكاسب ومكافآت لهم، فوصول شبكات الأخبار إلى زعماء الإرهاب تعد من أهم الأمور، التي تحتاجها المنظمات الإرهابية، وخير مثال على ذلك المقابلة التي بثتها قناة "سي إن إن" في مايو عام ١٩٩٧م مع زعيم القاعدة «أسامة بن لادن» عن وسائل تموينه وقواعد تجنيد الإرهابيين، حيث استغل ابن لادن تلك المقابلة بذكاء، ونشر فكره، وحدد أهدافه، ووجه نداءً مغلَّفاً لجميع شباب العالم الذين تتراوح أعمارهم بين ١٥ و٢٥ عاماً، وبرر قتله لدافعي الضرائب الغربية لأنهم شركاء ـ كما قال ـ في دعم حكوماتهم، التي تسيء إلى العالم الإسلامي وتحتل أراضيه وتدعم إسرائيل التي بدورها تقتل نساء وشيوخ وأطفال المسلمين وتهدم منازلهم على مرأى ومسمع من العالم.

ويبحث الإرهابيون على الدوام عن تفهم لقضاياهم التي يحاربون من أجلها؛ فرغم أن الغالبية من المشاهدين لا يتفقون مع تصرفاتهم الإرهابية وقتلهم للأبرياء؛ إلا أن فريقاً كبيراً منهم يتعاطفون مع قضيتهم، وخاصة عندما يعرضون المواقف الغربية واستخدام حق الفيتو من قبل أمريكا وبعض الدول الغربية ضد الحقوق الواضحة للعرب وللمسلمين بصورة عامة، وكذلك التصويت ضد قرارات الأمم المتحدة ومجلس الأمن لما تقوم به إسرائيل من ظلم وقهر وقتل للأطفال والنساء كما حدث في غزة وجنين ومن قبل في دير ياسين. والأمثلة من هذا النوع كثيرة، فقد استخدمت أمريكا حق الفيتو في الصراع العربي الإسرائيلي ٨٢ مرة ضد مشاريع قرارات تطرحها دول المنظمة الدولية، ٤٣ منها كانت اعتراضاً على مشاريع قرارات تدين إسرائيل. وصوتت ضد ١٠ قرارات تنتقد جنوب أفريقيا، وثمانية بشأن ناميبيا، وسبعة بشأن نيكاراغوا، وخمسة بشأن فيتنام. ولم تستخدم أي من الدول دائمة العضوية في مجلس الأمن الفيتو لمنع صدور قرارات تدين إسرائيل باستثناء أمريكا، وهو الأمر الذي تستغله كثير من المنظمات، حتى التي ليس لها علاقة بقضية فلسطين لتبرير هجومهم على مصالح أمريكا.

وفي إحصائية نشرت في مواقع عدة في شبكات الإنترنت، توضح أن أمريكا استخدمت حق الفيتو بإسراف على النحو التالي:

- في عام ١٩٦٧م استخدمت واشنطن الفيتو لأول مرة للحيلولة دون صدور نص قرار وقف إطلاق النار أثناء حرب يونيو وانسحاب القوات المتحاربة إلى خطوط الهدنة السابقة.

- في ٢٦/ ٧/ ١٩٧٣م اعترضت الولايات المتحدة على مشروع قرار تقدمت به الهند وإندونيسيا وبنما وبيرو والسودان ويوغسلافيا وغينيا، يؤكد على حق الفلسطينيين ويطالب بالانسحاب من الأراضي العربية التي احتلتها إسرائيل.

- في ٢٥/ ١/ ١٩٧٦م استعانت واشنطن بحق الفيتو لمنع قرار تقدمت به باكستان وبنما وتنزانيا ورومانيا ينص على حق الشعب الفلسطيني في ممارسة حق تقرير المصير وفي إقامة دولة مستقلة وفقاً لميثاق الأمم المتحدة، وضرورة انسحاب إسرائيل من الأراضي المحتلة منذ يونيو١٩٦٧م، ويدين إقامة المستوطنات اليهودية في الأراضي المحتلة، وفي العام نفسه استخدمت الولايات المتحدة الفيتو ضد قرار تقدمت به مجموعة من دول العالم الثالث يطلب من إسرائيل الامتناع عن أية أعمال ضد السكان العرب في الأراضي المحتلة.

- ٢٩/ ٦/ ١٩٧٦م استخدمت الولايات المتحدة الفيتو ضد قرار تقدمت به كل من جويانا وباكستان وبنما وتنزانيا، يؤكد على حقوق الشعب الفلسطيني في تقرير المصير والعودة إلى وطنه، وحقه في الاستقلال والسيادة.

- وفي ٣٠/ ٤/ ١٩٨٠م استخدِمَ الفيتو الأميركي ضد مشروع قرار تقدمت به تونس ينص على أحقية الشعب الفلسطيني لممارسة حقوقه المشروعة.

- في ٢٠/ ١/ ١٩٨٢م استخدمت الولايات المتحدة الفيتو ضد مشروع قرار يقضي بفرض عقوبات على إسرائيل لضمها مرتفعات الجولان السورية.

- وفي ٢٥/ ٢/ ١٩٨٢م استخدمت الولايات المتحدة الفيتو على مشروع قرار أردني يطالب السلطات المحلية في فلسطين بممارسة وظائفها، وإلغاء كل الإجراءات المطبقة في الضفة الغربية. وآخر في ٢/ ٤ من العام نفسه، لإبطال مشروع قرار يدين إسرائيل في محاولة اغتيال رئيس بلدية نابلس بسام الشكعة. وفي ٢٠/ ٤ من العام نفسه استخدمت الولايات المتحدة الفيتو ضد مشروع قرار عربي بإدانة حادث الهجوم على المسجد الأقصى.

- وفي ٩/ ٦/ ١٩٨٢م استخدمت الولايات المتحدة الفيتو ضد مشروع قرار اسباني بإدانة الغزو الإسرائيلي للبنان. وفيتو آخر في ٦/٢٥ من العام نفسه ضد مشروع قرار فرنسي في مجلس الأمن بشأن الاجتياح الإسرائيلي للبنان. كما عرقلت في ٨/٦ من العام نفسه صدور قرار يدين إسرائيل جراء سياستها التصعيدية في منطقة الشرق الأوسط، وتحديداً في لبنان.

- وفي ١٥/ ٢/ ١٩٨٣م صوتت الولايات المتحدة ضد قرار يستنكر مذابح مخيمي اللاجئين الفلسطينيين في "صبرا وشاتلا" بلبنان.

- في ٦/ ٩/ ١٩٨٤م صوتت الولايات المتحدة ضد إصدار قرار يؤكد أن نصوص اتفاقية جنيف الرابعة لعام ١٩٤٩م لم تطبق على الأقاليم المحتلة في لبنان بسبب استخدام أمريكا حق الفيتو.

- في ١٢/ ٣/ ١٩٨٥م استخدمت الولايات المتحدة الفيتو ضد مشروع قرار لبناني في مجلس الأمن يدين الممارسات الإسرائيلية في الجنوب اللبناني. وفي ١٣/ ٩ من العام نفسه استخدمت واشنطن الفيتو لإعاقة مشروع قرار أمام مجلس الأمن يدين الممارسات الإسرائيلية القمعية ضد الفلسطينيين.

- في ١٧/ ١/ ١٩٨٦م عرقلت الولايات المتحدة بالفيتو مشروع قرار في مجلس الأمن يطالب إسرائيل بسحب قواتها من لبنان، وكذلك في ٣٠/ ١ من العام نفسه استخدِمَ الفيتو الأمريكي ضد مشروع قانون لمجلس الأمن يدين الانتهاكات الإسرائيلية لحرمة المسجد الأقصى ويرفض مزاعم إسرائيل باعتبار القدس عاصمة لها. وفي ٧/ ٢ من العام نفسه استخدم الفيتو الأمريكي في مجلس الأمن لمنع إصدار قرار يدين اختطاف إسرائيل لطائرة الركاب الليبية.

- في ٢٠/ ٢/ ١٩٨٧م اعترضت الولايات المتحدة بالفيتو على قرار يستنكر سياسة «القبضة الحديدية» وسياسة تكسير عظام الأطفال الذين يرمون الحجارة خلال الانتفاضة الأولى.

- في ١٨/ ١/ ١٩٨٨م استخدمت واشنطن الفيتو ضد مشروع قرار في مجلس الأمن يستنكر الاعتداءات الإسرائيلية على جنوب لبنان ويطالبها بوقف أعمال التعدي على الأراضي اللبنانية والإجراءات ضد المدنيين. وفي ١/ ٢ من العام نفسه استخدمت الولايات المتحدة الفيتو ضد اقتراح في مجلس الأمن يطالب بالحد من عمليات الانتقام الإسرائيلية ضد الفلسطينيين في الأراضي المحتلة. وتكرر في ١٥ أبريل من العام نفسه صدور فيتو أميركي ضد قرار لمجلس الأمن يدين إسرائيل لاستخدامها سياسة القبضة الحديدية تجاه الانتفاضة الفلسطينية في الأراضي المحتلة في أعقاب طردها ثمانية فلسطينيين. وآخر في ١٠/ ٥ لنقض مشروع قرار في مجلس الأمن الدولي لإدانة الاجتياح الإسرائيلي لجنوب لبنان. وفي ١٤/ ١٢

استخدمت الولايات المتحدة الفيتو لمنع استصدار قرار من مجلس الأمن الدولي بإدانة الاعتداء الإسرائيلي الجوي والبري على الأراضي اللبنانية.

- وفي عام ١/ ٢ / ١٩٨٩م أوقفت الولايات المتحدة باستخدامها الفيتو جهود مجلس الأمن لإصدار بيان يرفض ممارسات إسرائيل في الأراضي الفلسطينية المحتلة ويدعوها إلى الالتزام باتفاقية جنيف الخاصة بحقوق المدنيين في زمن الحرب. وفي ١٨/ ٢ صدر فيتو أمريكي ضد مشروع قرار في مجلس الأمن الدولي بإدانة إسرائيل لانتهاكات حقوق الإنسان في الأراضي العربية المحتلة. وفي ٩/ ٦ فيتو أمريكي ضد مشروع قرار لدول عدم الانحياز يدين إسرائيل لسياستها القمعية في الأراضي المحتلة. وفي ٧/ ١١ اعترضت الولايات المتحدة بالفيتو على قرار قدم لمجلس الأمن يدين الممارسات الإسرائيلية في الأراضي المحتلة.

- وفي ١/ ٦/ ١٩٩٠م كان هناك فيتو أميركي ضد مشروع قرار في مجلس الأمن الدولي تقدمت به دول عدم الانحياز بإرسال لجنة دولية إلى الأراضي العربية المحتلة لتقصي الحقائق حول الممارسات القمعية الإسرائيلية ضد الشعب الفلسطيني.

- في ١٧/ ٣/ ١٩٩٥م يفشل مجلس الأمن بسبب الفيتو الأمريكي في التوصل إلى قرار يطالب إسرائيل بوقف قراراتها بمصادرة ٥٣ دونماً (الدونم يعادل ألف متر مربع) من الأراضي العربية في القدس الشرقية .

- في ٧/ ٣/ ١٩٩٧م أعاقت واشنطن صدور قرار يطالب إسرائيل بوقف أنشطتها الاستيطانية في شرق القدس المحتلة. وفي ٢١/ ٣ استخدمت الولايات المتحدة حق الفيتو عندما اعترضت على مشروع قرار يدين بناء إسرائيل للمستوطنات اليهودية في جبل أبو غنيم شرق مدينة القدس المحتلة.

- في ٧٢/ ٣/ ٢٠٠١م استخدمت الولايات المتحدة الفيتو لمنع مجلس الأمن من إصدار قرار يسمح بإنشاء قوة مراقبين دوليين لحماية الفلسطينيين في الضفة الغربية وغزة. وفي ١٤/ ١٢ أجهضت مشروع قرار يطالب بانسحاب إسرائيل من الأراضي الخاضعة للسلطة الفلسطينية، ويدين التعرض للمدنيين.

- وفي ٢٠/ ١٢/ ٢٠٠٢م أحبطت واشنطن مشروع قرار اقترحته سورية لإدانة قتل القوات الإسرائيلية عدة موظفين من موظفي الأمم المتحدة، فضلاً عن تدميرها

المتعمد لمستودع تابع لبرنامج الأغذية العالمي في الأراضي الفلسطينية المحتلة في نهاية نوفمبر.

- في ١٦/ ٧/ ٢٠٠٣م استخدمت أمريكا الفيتو ضد مشروع قرار لحماية الرئيس الفلسطيني ياسر عرفات عقب قرار الكنيست الإسرائيلي بالتخلص منه. وفي ١٤/ ٧ صدر فيتو أمريكي ضد قرار يطالب بإزالة الجدار العازل، الذي تبنيه إسرائيل والذي يقوم بتقطيع أراضي وأوصال السلطة الفلسطينية، وينتهك أراضي المواطنين الفلسطينيين .

- وفي ٢٥/ ٣/ ٢٠٠٤م صوتت الولايات المتحدة لإسقاط مشروع قرار يدين إسرائيل على قيامها باغتيال مؤسس حركة المقاومة الإسلامية (حماس) الشيخ «أحمد ياسين». وفي ٥/ ١٠ أسقطت واشنطن مشروع قرار يطالب إسرائيل بوقف عدوانها على شمال قطاع غزة والانسحاب من المنطقة.

- في ١٣/ ٧/ ٢٠٠٦م فشل مجلس الأمن في تبني قرار يطالب بإطلاق سراح الجندي الإسرائيلي المحتجز من قبل الفصائل الفلسطينية المسلحة مقابل إطلاق سراح الأسرى الفلسطينيين في سجون الاحتلال، ويطالب بوقف الحصار والتوغل الإسرائيلي في قطاع غزة ، وذلك بسبب تصويت الولايات المتحدة ضد القرار.

وكنتيجة حتمية لهذا الظلم والقهر المنصب على العالم الإسلامي، الذي تمارسه إسرائيل وتحميه واشنطن، بغطاء سياسي وعسكري بالإضافة إلى تدخل أمريكا وحلفائها الغربيين، في كل من العراق وأفغانستان؛ فإنه من البديهي أن تظهر قوى تكافح وتقاتل بهدف الانتصار للمستضعفين على حد تعبيرهم. ولا شك أن إدعاءاتهم ستلقى آذاناً صاغية؛ بل أنها ستجد من سيضحي بحياته من أجلها؛ وخاصةً عند ما تنشر صور القتل والتعذيب وهدم المنازل في غزة وفلسطين بوجه عام، وضحايا التعذيب في أبو غريب، والأفغان الذين نقلوا في حاوية مغلقة ليجدوا حتفهم بسبب نقص الأكسجين وحرارة الشمس داخل الحاوية، وما حصل من ظلم وتعذيب لآخرين في جوانتانامو، وما قامت به شركة «بلاك ووتر» الأمريكية من قتل لعراقيين أبرياء؛ ناهيك عن الاغتصاب والنهب، الذي يتم تحت نظر العالم وسمعه في جميع المناطق التي تخضع للحماية الغربية. ويعتقد الإرهابيون أن المجتمع يحتاج لمساعدتهم لتفهم وقبول عدالة قضيتهم، وأن العمليات، التي يقومون بها من وجهة نظرهم هي الوسيلة الوحيدة الممكنة لقمع قوى

الشر العظمى. كما أن العلاقات الجيدة بينهم وبين الإعلام في غاية الأهمية، وكثيراً ما يحرصون على تنمية وتطبيع هذه العلاقة على فترات زمنية طويلة، ويسعون كذلك إلى تنمية متعاطفين معهم في مواقع إعلامية، كما يسيطرون أحياناً على منظمات إخبارية صغيرة عن طريق تمويلها مادياً.

وهم يعملون بجد لتنمية الشرعية لقضاياهم، ويسعون من أجل أن يعطيهم الإعلام غطاء شرعياً لما يوصف في العادة بأنه عداء فكري أو شخصي مع المجاميع المسلحة والأحزاب السياسية المرتبطة بهم، التي تدافع عن القضية. فإسرائيل، على سبيل المثال، تمارس الإرهاب عن طريق مجاميع إرهابية سرية، مثل المستوطنين وغيرهم، وتعطيهم الغطاء الشرعي عن طريق الأحزاب السياسية المتعددة مثل إسرائيل بيتنا، وحزب كاديما، وغير ذلك من الأحزاب. ويمكن قول الشيء نفسه عن الجيش الجمهوري الإيرلندي، حيث إن «جاري آدم» يقوم بدور السياسي في «الشينفين» ويدير الإرهاب في منظمة الجيش الجمهوري الإيرلندي، وكذا الحال في حزب الله بجناحيه السياسي والمسلح، ليس هذا فحسب؛ بل إن الإرهابيين يسعون كذلك للحصول على اهتمام الصحافة بوجهات نظر المنظمات غير الحكومية، التي ينشئونها والاعتراف بها، وبالدراسات التي تنشرها هذه المنظمات، والتي تعمل كغطاء لتجنيد الشباب وترحيلهم إلى الدولة المستهدفة.

وأثناء الاختطاف يحتاج المختطفون إلى تفاصيل عن الشخصيات المختطفة وعن قيمتهم الاجتماعية، وتفاصيل عن محاولات الإنقاذ التي تحت الإجراء، وتفاصيل ما تم نشره للمجتمع عن عمليتهم؛ وخاصة عندما تكون العملية ممولة من قبل الحكومة، مثل تدمير غزة والقتل الجماعي للأطفال والنساء من قبل الجيش الإسرائيلي والمرتزقة عام ٢٠٠٦م أمام مسمع ومرأى من العالم بحجة الثأر من شبه الصواريخ، التي تطلقها حماس على مناطق غير مأهولة من جنوب إسرائيل. وتريد المنظمات الإرهابية تغطية إعلامية عن الأضرار التي سببتها لأعدائها؛ وخاصة عندما يكون المنفذون للعملية وأسباب الهجوم غير واضحة، فهم يحتاجون إلى نشر الرعب وتضخيمه بين المواطنين من قبل الإعلام لتحقيق خسائر اقتصادية، كأن يخيفوا المستثمرين والسياح، كما يحدث في مصر ولبنان واليمن، وما يقوم به اليهود في فلسطين وجعل المواطنين يفقدون الثقة في حكوماتهم، ويوضحون عدم قدرة الدولة على حماية مواطنيها.

ولتحقيق تكامل أفضل بين الحكومات والإعلام؛ تسعى الحكومات لفرض تفهم وإدراك وتعاون وتقييد وولاء من الإعلام في محاولات للحد من أضرار الإرهاب للمجتمعات، وبذل جهود حثيثة لمعاقبة أو اعتقال المتورطين في الأعمال الإرهابية[١٩]. لذا تسعى الحكومات باستمرار إلى تغطية إعلامية لنشر وجهات نظرها فيما يتعلق بالإرهاب، والتعتيم بقدر الإمكان على وجهات نظر المنظمات الإرهابية، وتتوقع الحكومات من وسائل الإعلام دعم ما تقوم به من إجراءات أثناء عملياتها. ونشر المعلومات والتصريحات، التي تسمح بنشرها الجهات الحكومية، التي تعالج المشكلة عندما يكون في ذلك مصلحة أمنية، لتوضيح الأهداف والسياسات الحكومية، أو على أقل تقدير، تقديم تقارير متوازنة كأن توضح أن نقاش الحكومة مع الإرهابيين لا يعني استسلامها لمتطلباتهم.

ومن أهم أهداف الحكومة إبعاد المنظمات الإرهابية عن وسائل الإعلام، وذلك لمنع استفادتها من استخدام المنابر الإعلامية، إلا إذا كان ذلك سيؤدي إلى هزيمة الإرهاب. وخير مثال على ذلك الدور الذي قامت به وسائل الإعلام للإطاحة بإرهابي الجامعات ثيودور كازينسكي Theodore Kaczynski المعروف آنذاك باسم مفجر الجامعة «Unabomber»، وقد شاع هذا الاسم والطريقة واستخدم في إيطاليا وجرائم أخرى، وأدى إلى هزيمة المجرمين، وخاصة الذين كانوا يبحثون عن الشهرة أو الانتقام. وهناك هدف آخر لدى الحكومات؛ وهو توجيه الإعلام لإظهار المنظمات الإرهابية على أنها عصابات إجرامية والابتعاد عن تمجيد أفعالهم وجرائمهم، أو تبني وجهات نظر الإرهابيين عند اختطاف المسؤولين أو تفجير المباني أو اختطاف الطائرات، بصرف النظر عن المبادئ التي يدعيها الإرهابيون.

أما في حالة عمليات تخليص الرهائن؛ فإن الحكومات تعمل على إبعاد وسائل الإعلام والجماهير عن موقع الحدث، مع أنها ترغب أن تقدم الصحافة كل ما تعرفه أو تستطيع الوصول إليه من معلومات عن المختطفين. ومن أهم الأهداف التي تسعى إليها الحكومات باستخدام أسلوب التشهير والنشر، هو المساعدة في إخماد التوتر لضمان هدوء المجتمع. وتعتقد الحكومات أنه من المفيد الابتعاد عن نشر المناظر ومقاطع الفيديو المؤثرة مثل تصوير الأمهات أو أقارب المختطف وهن يبكين وينتحبن، لأن مثل هذه

المناظر تجعل المجتمع يضغط على الحكومة للتنازلات والاستسلام لمتطلبات المجرمين. ومن الضروري ـ أيضاً ـ أن تبتعد وسائل الإعلام عن نشر المعلومات المتعلقة بالخطط التي تتبعها الحكومة للسيطرة على الموقف والإسهام في عزل المختطفين عن المعلومات التي تساعدهم على رفع مستوى الضرر. ومن الضروري أيضاً أن تحجم وسائل الإعلام عن نشر أسرار الدولة المتعلقة بالعمليات، التي نفذتها ضد حوادث الإرهاب؛ وخاصة الإجراءات التقنية التي ربما تنشرها وسائل الإعلام بهدف توضيح مستوى النجاح الذي حققته الحكومة أو النجاح الذي حققه الإرهاب باستخدام تقنيات حديثة، والتي توضح الأساليب التقنية التي استخدمتها الحكومة أو الإرهاب، وذلك تفادياً تقليده من قبل منظمات أخرى ليس لها خبرة بتلك التقنيات. وعلى سبيل المثال ما تداولته الصحف من أسباب فشل الإرهابي البريطاني «رتشارد ريد»، الذي أدين بمحاولة تفجير طائرة من خلال إخفاء متفجرات في حذائه عام ٢٠٠٣، وكذلك نشر تفاصيل محاولة النيجيري «عمر الفاروق عبدالمطلب»، لتفجير طائرة «إيرباص ٣٣٠» التابعة لشركة «دلتا أيرلاينز» الأمريكية خلال رحلتها بين أمستردام وديترويت في ٢٥ ديسمبر ٢٠٠٩م. ويلحظ أن تنظيم القاعدة في شبه جزيرة العرب تبنَّى هذه المحاولة قبيل خطاب للرئيس الأمريكي «باراك أوباما» حض فيه على تكثيف الجهود لمكافحة الإرهاب.

وقد يتسبب نشر معلومات التعاون بين الولايات الأمريكية وأي دولة إسلامية في إحراج كبير لتلك الدولة. ومن الأمثلة التي سببت إحراجاً لدول تعاونت مع الولايات المتحدة للقبض على قاتل الرهينة الأمريكية كانت دولة باكستان التي تعاونت للقبض على «مير أمل خانزي» المتهم بقتل رجل المخابرات المركزية وسمحت بنقله إلى الولايات المتحدة الأمريكية، وبعد أن نشرت وسائل الإعلام تفاصيل القبض على المتهم في يناير عام ١٩٩٧م ظهرت الصحف الباكستانية بحملة احتجاج على حكومتها بسبب التغاضي عن العملية وعدم تطبيق الدستور الباكستاني، وطالبت بتفسير من الحكومة لما حدث من تجاوزات دستورية وأهمها السماح لدولة أجنبية بالقبض على مواطن باكستاني ونقله خارج الدولة للمحاكمة[٢٠]. وكذلك ما أعلن في يناير عام ٢٠١٠م عن التعاون بين اليمن والولايات المتحدة للقضاء على فرع القاعدة المتمركز في اليمن، مما أثار الرأي العام اليمني بجميع أطيافه ومشايخه، الذين اعتبروا أن التدخل المباشر لأمريكا في اليمن يعد احتلالاً يستدعي الجهاد لمكافحته، مما اضطر

الحكومة اليمنية وأمريكا لإنكار أي تدخل مباشر من قبل القوات الأمريكية، وأن المساعدات اقتصرت على التدريب وتموين اليمن بالإمكانيات، التي تساعدها في مواجهة الإرهاب.

ويقع على الصحافة مسؤولية كبرى في تحري الدقة فيما تنشره من معلومات مغلوطة يصدرها أنصار الإرهابيين والمتعاطفين معهم، أو أي مستفيد من نشر المعلومات المغلوطة، فكثير من المجموعات لديها دوافع لنشر معلومات خاطئة، مثل طريقة تفجير طائرة، أو الإعلان عن الجهة المسؤولة عن ذلك. كما تريد الحكومات من الإعلام تعزيز ودعم صورة إداراتها وخاصة المعنية بمكافحة الإرهاب، وكثيراً ما تسرب الحكومات للإعلام معلومات بطرق محكمة ومتقنة، لتوجيه المصادر الإعلامية لتفهم الإجراءات وعدم انتقادها، وتطالب الحكومات من المراسلين إبلاغهم عن أي معلومات، يعتقدون أنها مؤكدة عن نية المنظمات الإرهابية من تنفيذ عمليات إرهابية، أو التخطيط لها أو عند حصولهم على معلومات تتعلق بتورط شخص أو أشخاص في مساعدة الإرهاب.

وفي حالات قصوى عندما تسمح الظروف، وعندما يتعرض الأمن الوطني للخطر، وعندما تكون فرص النجاح عالية؛ فإن الحكومة قد تتجه لطلب التعاون مع الإعلام لطرح حيلة أو ذريعة تسهم في تحييد التهديدات المباشرة من الإرهاب. وفي حالات التعامل مع القضايا الإرهابية التي تشكل جرائم شنيعة؛ فإن التعاون بين الحكومة والإعلام أمر شائع، ومن أمثلة ذلك عدم نشر أدلة حصل عليها المراسل في مسرح الجريمة، أو مساعدة الأمن بنشر معلومات غير حقيقية لتوريط الفاعلين للجريمة، كأن يطمئنوا المجرم أنه بعيد عن متابعة الأمن وأنه في مأمن عنهم وأن الشبهة متجهة لناحية أخرى.

أما المراسلون والإعلاميون؛ فإنهم يحتاجون إلى حرية النشر وتغطية الأحداث دون أي قيود خارجية، سواءً أتت من ملاك الوسائل الإعلامية، أو المعلنين التجاريين، أو الحكومات، أو محرري الصحف. ويسعى الإعلام إلى تحقيق ما ينشده الجمهور من التزود بمعلومات حقيقية، تلبي شغفه للحصول على المعلومات والخلفية الواضحة، التي تساعده على الإسهام في دعم التوجه العام، وللمشاركة في صنع مجتمع متطور يعمل ويتفاعل بالتوازي مع بقية أدوات الدولة ومؤسساتها. ومما يعرقل الانسجام التام بين الإعلام وتطلعات الحكومات في التعاون المثمر، أن جميع وسائل الإعلام تحاول تحقيق السبق في نشر القصص والأحداث؛ لأن

الأخبار القديمة ليست أخباراً جذابة، والضغوط التي تمارس على الإعلام لنشر وتحرير أخبار في حينها تزداد بفعل التقدم التقني الهائل في وسائل نقل المعلومات وبيئة الإنترنت. وتسعى وسائل الإعلام لنشر وبث الموضوع في حينه، وجعله مثيراً بأقصى ما يمكن، ولهذا فإنها عادةً ما تدعم ذلك بمقابلات مع المعنيين بالحدث، وكثيراً ما ينتج عن ذلك بعض الإسقاطات التي تعرقل النجاح، وربما تفشل عمليات الإنقاذ في أحيان أخرى. فعلى سبيل المثال اتهم «مايكل بيرتش» الناطق الرسمي لوزارة الدفاع الأمريكية في ١٩ يونيو عام ١٩٨٥م وسائل الإعلام الأمريكية بأنها وفرت معلومات عن التحركات السياسية والعسكرية، التي استفاد منها حزب الله عند اختطافهم رحلة شركة TWA رقم ٨٤٧، التي أقلعت من أثينا متجهة لروما، عندما أذاعت محطة تلفزيون ABC معلومات عن تحرك قوة التدخل السريع «دلتا» إلى الجزائر، مما تسبب في إنهاء النقاش مع الخاطفين وقتل سائق البحرية «روبرت ستيثام»، وأخذ جميع طاقم الطائرة ماعدا ثلاثة منهم واحتجازهم من قبل منظمة أمل وحزب الله حتى تم إطلاقهم.

ومعظم المراسلين يسعون لتحقيق المهنية والدقة في نقل الأحداث، بموضوعية محايدة وشفافية عالية متسلحين بقوانين حرية التعبير واحترام الرأي الآخر، من خلال الاستماع إلى وجهات النظر المختلفة، دون الاكتراث بإمكانية الانخداع من قبل مروجي المعلومات، التي تتسرب بتنسيق مع المنظمات التي أطلقتها. ويمكن القول أن الدقة والمهنية صعبة المنال؛ وخاصة عندما تتوافر جهود كبيرة ومنظمة للخداع من قبل المنظمات المستفيدة من ذلك. ويسعى الإعلام الحر الشامل على الدوام لحماية قدراته لكي يعمل بحرية وأمن في مجتمعه، ولذا فإنه في معظم الأحيان يتجاوز حاجته لتحقيق القدرات، ويطالب بحماية حقوقه القانونية للنشر دون أي قيود، وكذلك طلب توفير حماية مراسليه من الاعتداءات الجسمية، والتهديدات والتحرش، أو الاعتداء العنيف خلال العمليات، وكذلك الحماية من الاغتيالات المحتملة من قبل الإرهابيين، كنوع من الثأر عند نشرهم تقارير تسيء إليهم. والإعلاميون يتسلحون باستمرار بمنهجية حماية حقوق المجتمع في معرفة الحقيقة، ويرون أن تحقيق ذلك يتم بالتغطية الإعلامية الصادقة والدقيقة والمثيرة، مثل نقل ونشر ردود الفعل العاطفية والانفعالية للضحايا وأقاربهم وردود فعل شهود العيان والمواطنين في الشارع، ودفاع الجهات المتهمة بالإرهاب عن أنفسهم، وإظهار تبريراتهم وتوضيح قضاياهم، وقد يصل ذلك إلى حد نشر معلومات تم التحفظ عليها من قبل الجهات الأمنية والحكومية. وليس لدى المراسلين أي اعتراض للقيام

بدور إيجابي لحل جزئية محددة من الحالة الإرهابية، إذا كان ذلك لا يؤثر على الإثارة والقيمة للقصة أو الحالة المراد نشرها.

وتدل العديد من الأنشطة الإرهابية على نشوء اتجاه يؤثر على العلاقة بين الإعلام والإرهاب والحكومات، مثل عدم ادعاء المنظمات الإرهابية مسؤوليتها عن بعض الحوادث الإرهابية، وترك الفاعل مجهولاً والتوجه نحو أعمال إرهابية أكثر وحشية وشناعة، والاعتداء على المراسلين والمنظمات الإعلامية.

وقد يرى المتابع اليوم، أن كثيراً من الحوادث المجهولة المصدر، لا يدعي أحد مسؤوليته عنها، ولا يتبعها أي مطالب من قبل أي منظمة إرهابية، من ذلك ما حصل في بدايات كارثة مركز التجارة الدولي في نيويورك في ١١ / ٩، مما أعطى للإعلام دوراً أوسع في التخمين ومحاولة معرفة الفاعل الحقيقي، وأسباب وأبعاد هذا الفعل. ولا شك أن مجهولية الفاعل مما يمنح وسائل الإعلام الحصانة لتضخيم الأمور، ويفسح المجال للمزيد من التوقعات والدوافع والمحفزات، التي تُؤدي لمثل هذا الفعل، وهذا يعطي الإعلام حرية كبيرة ومدى واسعاً لكتابة التقارير الصحفية، وإطلاق العنان للتصورات والافتراضات، التي كثيراً ما تصل إلى أقصى مستويات الخيال، وتظهر كثير من التقارير والكتب التي هي أقرب للخيال منها للواقع. ولا يخفى على أحد ما تسببه التغطية الإعلامية من رعب وشوشرة على العامة، تؤدي أحياناً في أن تقوم الحكومات بردود فعل ضد مصالح مواطنيها، وضد الديمقراطية، وتعمل على خفض سقف الحرية، وحرية الحركة، وعرقلة التنقل، ووضع قوانين للتفتيش، التي تؤخر وتضايق المسافرين في البر والجو والبحر، ومداخل الفنادق والمؤسسات الحكومية المهمة التي يحتاج المواطن مراجعتها.

وفي سياق ومحيط التقدم الهائل في تقنية المعلومات، لا يمكن إهمال توجه المنظمات الإرهابية لعمليات إرهابية عنيفة، ورفع سقف العنف الإرهابي[٢١] مما تسبب في خفض نجاحات الإرهاب الدولي بصورة عالية خلال العشر سنوات الماضية، إلا أن مستوى القتل قد ازداد، وأن سمة الحوادث الإرهابية مستمرة في ازدياد الوحشية، ضد الأهداف المدنية، التي تؤدي إلى قتل أكبر عدد ممكن من الأبرياء باستخدام أساليب تفجير متقدمة. ومع شروق شمس كل يوم تزداد خشية العالم من تمكن المنظمات الإرهابية من حصولها على أسلحة الدمار الشامل

مثل الأسلحة الحيوية، أو الكيميائية، أو النووية. وكلما ازدادت وحشية الإرهاب وعنفه يزداد اتهام الإعلام بالمسؤولية عن هذه الزيادة إلى حد كبير، وذلك لأنه يسبب تحقيق الكثير من أهداف المنظمات الإرهابية بتضخيم تأثير الأحداث. ومن أخطر ما يواجه الإعلام، الهجوم على المراسلين الإعلاميين والمؤسسات الإعلامية، فقد بدأ الهجوم على المراسلين الصحفيين يتزايد، وخاصة المؤثرين منهم، حيث لوحظ تزايد حالات تصفية المراسلين، كما هو الحال في لندن وروسيا والمكسيك والعراق وباكستان وغيرها. وهناك حالات ـ أيضاً ـ في واشنطن ونيويورك، كما حصل في مبنى الأمم المتحدة ومبنى الإعلام الوطني. وحسب ما جاء في تقرير منظمة حماية الصحفيين CPJ أن عدد الصحفيين الذين قتلوا منذ عام ١٩٨٦م وصل إلى حوالي ٣٠٠ شخص وفي عام ١٩٩٥ فقط بلغ عددهم ٤٥ شخصاً[٢٢].

الباب الثاني

تهديدات البنية التحتية

الفصل الأول

نبذة تاريخية: مخاطر البنية التحتية قديماً وحديثاً

الفصل الأول

نبذة تاريخية: مخاطر البنية التحتية قديماً وحديثاً

البنية التحتية ضرورة من ضروريات التقدم الحضاري، التي لا يستغني عنها المواطن، بحيث يعد إنشاؤها وتطويرها من أهم واجبات الدول. والهدف من الإنشاءات هذه، تسهيل حياة المواطنين وتنقلاتهم ونقل محاصيلهم ومنتجاتهم الزراعية والصناعية، وتسهيل التعاملات التجارية والتبادلات المعلوماتية بين الدول، ولهذا فإنه؛ من المستحيل حصر الاستفادة من البنية التحتية لاستخدامات الخير، ومنع المخربين واللصوص والقراصنة من استخدامها لأغراض الشر. وكلما تطورت الإمكانات البشرية وسهلت وسائل الحياة، باستخدام التطور التقني سهل على قوى الشر استخدام تلك الإمكانات لتحقيق أهدافهم العدوانية. وهذا الأمر ليس مرتبطاً بالحاضر فقط؛ بل إن إساءة استخدام البنية التحتية قد بدأ مع فجر التاريخ. فلو نظرنا إلى أعظم ما شيده الإنسان في العالم القديم، وهو البنية التحتية للطرق والقنوات التي بناها الرومان، منذ ٣٠٠ عام قبل الميلاد، والتي وصلت إلى حوالي ٥٠,٠٠٠ ميل من الطرق الصلبة السريعة ولا زال بعضها موجوداً إلى اليوم[٢٣]. ومع أن تلك الطرق أنشئت في ذلك التاريخ لتلبية الاحتياجات العسكرية؛ إلا أنها استخدمت أيضاً للتجارة والزراعة ونقل البريد، مما يسر تأسيس وإدارة الحكم الروماني في إمبراطوريتهم الشاسعة. وعندما استشعر الرومان أن الإنتاج الصناعي للاستهلاك غير المحلي كان يواجه صعوبة بسبب رداءة النقل والقناطر وغياب الأمن، ولكون العربات التي تجرها الثيران بطيئة، والنزل في الطرق نادرة، وتزايد أعداد

اللصوص، اضطرت لبناء القلاع وسيرت فرق المراقبة لحماية بنيتها التحتية، ووجهت حركة النقل في معظم البلاد إلى القنوات والأنهار، وركزت على الطرق البحرية والسفن لاستيراد وتصدير حاجتها من البضائع؛ فبدأت بمشروع طموح حتى بالمعايير الحديثة، واستفادت منه في النقل، وهو نظام القنوات، حيث نقلت المياه إلى المدن للاستخدامات العامة والخاصة، كما أنها وفرت المياه للزراعة والنظافة. وأسهمت البنية التحتية الرومانية المتطورة بجدارة في الازدهار



شكل (٤): نقل المياه من قناة تارا غون

والنمو الاقتصادي، الذي يعد من الصفات المميزة للحضارة الرومانية القديمة، وما أن حلت سنة ٢٠٢ ق. م حتى كان الرومان قد أنشأوا ثلاثة من الطرق «القنصلية العظيمة». وسميت قنصلية، لأنها كانت تسمى عادة باسم القناصل الذين كانوا يبدأونها، وما لبثت هذه الطرق العامة أن فاقت في متانتها واتساعها الطرق الفارسية وطرق قرطاجنة، التي اتخذها الرومان نماذج لهم في بادئ الأمر. وكان أقدم هذه الطرق، كما جاء في أدبيات العصر الروماني وتاريخ الأمم القديمة، هو طريق ڤيا أبيا الذي يصل روما كابوا Capua وبدأه «أبيوس كلوديوس Appius Claudius»، وكان كفيف البصر في عام ٣١٢ ق. م وكذلك طريق ڤيا لاتينيا via Latina الذي خرج به الرومان حوالي عام ٣٧٠ ق.م إلى تلال الألبان، ثم جرى تمديده فيما

بعد ليبلغ طوله ٣٣٣ ميلاً إنجليزياً، وأصبح يربط ساحلي شبه الجزيرة الشرقي والغربي. وقد يسرت تلك الطرق وغيرها التجارة مع بلاد اليونان والشرق، كما كانت عاملاً كبيراً في توحيد إيطاليا. ثم توالى إنشاء الطرق في القرن التالي من إيطاليا إلى خارجها، مثل الطريق المؤدي إلى يورك، وفينا وثيسالونيكا Thessalonica ودمشق. كما امتدت الطرق على طول ساحل إفريقية الشمالي وأسهمت هذه الطرق في الدفاع عن الإمبراطورية وتوحيدها وبعث الحياة فيها، وذلك بتسهيل تحركات الجيوش ونقل الأخبار والثقافات والأفكار في ربوعها، كما أضحت مسالك عظيمة للتجارة، وكان لها شأن في إعمار إيطاليا وأوربا وزيادة ثرائهما. ومع كل هذا لم تزدهر التجارة في إيطاليا، كما هو الحال في شرقي البحر الأبيض المتوسط، وذلك بسبب الثقافة السائدة في إيطاليا التي تحقر الانخراط في البيع والشراء، ونظرة المجتمع بعين الاحتقار إلى الشراء بأثمان بخسة والبيع بأثمان مرتفعة.

أما في الريف، فقد كان الأهالي يكتفون بالأعياد التي تقام من حين إلى حين، وبأسواق اليوم التاسع في المدن، وهذا يؤكد مدى العلاقة الوثيقة بين ثقافات الشعوب والنمو التجاري والصناعي، فعلى سبيل المقارنة، نجد أن بعض قبائل الجزيرة العربية عزفت عن الصناعة في حقبة من التاريخ، وكانت تنظر إليها بوصفها من وسائل الحياة لدى قبائل الغجر وغيرهم من الذين لا ينتمون للقبائل المشهورة، مما أسهم في تخلفهم عن ركب الثورة الصناعية. كما أن التجارة الخارجية في إيطاليا - أيضاً - لم تبلغ شأناً عظيماً بسبب خطورة النقل البحري، وصغر حجم السفن الشراعية، التي لا تزيد سرعتها عن ستة أميال في الساعة. وكذلك كانت قرطاجنة تسيطر على غربي البحر الأبيض المتوسط، والممالك الإغريقية تسيطر على شرقه. وكان القراصنة ينقضُّون من مكامنهم من حين إلى آخر على السفن التجارية. وكان انسداد نهر التيبر، قد زاد في عرقلة النمو الاقتصادي لإيطاليا، بسبب تراكم الطمي وسد مدخل الميناء عند أستيا Ostia. كما أن شدة التيارات النهرية تضيف مشقة وتكاليف مالية لسير السفن المتجهة عكس التيار، مما لا يبرر حجم العوائد المالية المتوقعة. ونهر التيبر، ويسمى بالإيطالية «Tevere»، هو ثاني أطول نهر في إيطاليا، يبدأ في سلسلة جبال توسكان ويتدفق جنوبا لمسافة ٤٠٥ كيلاً، وفي نهايته يعبر مدينة روما قبل أن يصب في البحر الأبيض المتوسط في منطقة أوستيا، وكان يعد وسيلة تجارة مهمة في العهود الرومانية. لهذا بدأت السفن حوالي عام ٢٠٠ ق.م ترسو عند بتيولي على بعد مئة وخمسين ميلاً جنوبي روما، ومنها تنتقل حمولتها براً إلى العاصمة.

ومع كل فوائد تلك المشاريع العملاقة الكثيرة والواضحة، إلا أن هذه البنية التحتية أوجدت ثغرات أمنية جديدة وخطيرة، إذ إنها وفرت طرقاً للمهاجمين تمكنهم من الوصول بسهولة للمدن الرومانية، التي أصبحت هدفاً للهجوم المباشر من اللصوص والقراصنة



شكل (٥): طريق روماني في Pompeii

وأعداء الإمبراطورية. ونتيجة لذلك استثمر الرومان بثقل كبير في تشييد القلاع والجدران الحصينة الواقية والتحصينات الأخرى على طول طرقهم ومن حول مدنهم، وسنوا القوانين والمراسيم التي تهدف إلى حماية البنية المتعلقة بالطرق وقنوات الري.

واليوم، نجد أن البنية التحتية العالمية، كما هو الحال في المملكة العربية السعودية، أيضاً أعجوبة هندسية؛ بل إن هناك من يعدها خيالاً تقنياً يتحقق، فشبكات الإنترنت أصبحت وسيلة مهمة لتبادل الأخبار والمعلومات والاتصال السريع بين جميع فئات المجتمع، بما فيهم القراصنة والإرهابيين. وتحمل شبكات الهواتف يومياً مئات الملايين من المكالمات والرسائل الإلكترونية، كما أن الشبكات المالية المحلية والعالمية تنفذ تعاملات اقتصادية تصل في قيمتها إلى تريليونات الدولارات، وشبكات الطاقة الكهربائية تخدم ملايين المستهلكين بنقل ملايين

الكيلوات من الطاقة الكهربائية إلى أي مكان. وتعد قطاعات البنية التحتية المختلفة مثل قطاع النقل وقطاع المال والبنوك وقطاع الطاقة وقطاع الاتصالات، القوة الدافعة للحياة الحديثة في العالم بأسره.

والبنية التحتية العالمية أعظم من مجرد نسخة أكبر وأحدث وأكثر تعقيداً من شبكة الطرق وقنوات الري الرومانية، والسبب أن لها مميزات أساسية وفي غاية الأهمية، ولأنها تعمل آلياً ومعظم عملياتها ممكننة أو مؤتمتة. وتعدت المكننة مجالات الأعمال الخاصة والمصانع إلى مكننة كافة المعاملات الإدارية في دوائر ومصالح الدول، وانصبّت الجهود في مشاريع «خطط تطوير الأداء» لمصالح الحكومة، التي تخدم المجتمع في جميع حكومات العالم الحديث، وظهر اصطلاح «الحكومة الإلكترونية أو التعاملات الحكومية» بالإضافة إلى مصطلحات «المكننة والأتمتة». وتهدف مشاريع المكننة إلى تعزيز أداء مصالح الدولة، من خلال إعادة النظر في إجراءات العمل لتنظيمها وتيسيرها وتدريب الموظفين على الإجراءات الجديدة، إضافة إلى تفعيل النظام المعلوماتي واستكمال قاعدة البيانات وأرشفة المعلومات بشكل يسهل عمل المواطن ويقلص المهلة الزمنية اللازمة لإنجاز مختلف المعاملات.

وتدخل المكننة والأتمتة في جميع المجالات من توزيع آلي للمكالمات إلى توزيع الطاقة الكهربائية، ومن فصل آلي للطائرات إلى تحويلات إلكترونية للاعتمادات المالية والتحديد الآلي للمخزون والمؤن. ويتم تشغيلها بواسطة شبكات للمعلومات تعمل آلياً، وفي جميع القطاعات يعد الحاسوب جزءاً مكملاً لعمليات التشغيل، والتحكم في الأداء، وتنفيذ التعاملات والتبادلات بجميع أنواعها، وكذلك تكييف السعة الاستيعابية حسب الاحتياجات عن طريق وسائل الاتصالات بين عناصر الأنظمة المختلفة وتوصيل المعلومات لعناصر التشغيل البشرية. وهذا التوجه نحو المكننة الآلية بدأ تشييده منذ عقود، ولكنه بدأ يتزايد بدرجة مذهلة في السنوات القليلة الماضية. فالاعتماد على المكننة الآلية مطلب مهم وعملي هذه الأيام، بسبب التغير المستمر في بيئة العمل، حيث مكّن ترافق المكننة مع تقنية المعلومات مرافق الخدمات العامة من تقديم خدمات جديدة وتحسين الخدمات الموجودة. كما وفرا تشغيلاً واستخداماً أفضل للموارد بكفاءة عالية، وكذلك إمكانية تهيئة بيئة تنافسية عالية من خلال الاستجابة السريعة لطلبات جميع عملائهم. وتهيئ شبكات المعلومات سهولة فائقة للمدراء للوصول إلى فروع شركاتهم ومنظماتهم المنتشرة محلياً وإقليمياً وعالمياً، كما تمكنهم من تصميم خدماتهم

لتتناسب مع زبائن وعملاء معينين.

ومن الضروري النظر في ما إذا كان التبني السريع وواسع الانتشار لتقنية المعلومات مع جميع منافعها سيخلق «ثغرات أمنية» تؤدي إلى خفض «الاعتمادية» التي يتوقعها خبراء المجتمع في البنية التحتية الحديثة من عدمه. وفي كل يوم يتعطل فيه نظام معقد؛ تظهر التجربة أن العطل يحصل فجأةً وبالكامل. ومقولة «النظام معطل» أصبحت جملة مألوفة في بيئة الأعمال، التي تعتمد على الحواسيب لأداء مهامها مثل مكاتب الخطوط و«السوبر ماركت» ومكاتب تأجير السيارات. ومثل هذه الأمور المزعجة تعد أموراً يسيرة جداً إذا ما قورنت بالمشاكل المحتملة، التي يمكن أن تفاجئنا عند تعطل شبكات الحواسيب التي تساند البنية التحتية وأتمتتها على مستوى البلاد.

إن شبكات الحواسيب المعقدة، التي تعتمد عليها عمليات البنية التحتية بصورة متزايدة، معرضة للأعطال مثل أي نظام آخر من صنع الإنسان، لأن إخفاقات البشر في التصميم والبناء والتشغيل إضافةً إلى المسببات الطبيعية وتقدم العمر الزمني لأجزاء النظام والكوارث الطبيعية؛ كل هذا يؤدي إلى خفض واضح للاعتمادية. وأي من هذه العوامل، التي لا يمكن تلافيها يمكن أن يتسبب في قصور شامل لخدمات البنية التحتية العالمية. وبكل وضوح يمكن القول أن إمكانية الوصول عن بعد، رغم أهميتها لخدمة المستفيدين في أي نظام، تسبب ثغرة خطيرة تمكن قراصنة الحواسيب من الوصول إلى صلب النظام بهدف تعمد تعطيل خدمات أساسية، وذلك بالعبث في معلومات الشبكة التي تحمل أوامر التحكم والأتمتة في مرافق تقديم تلك الخدمات. ويمكن أن يتسبب مثل هذا الهجوم الإرهابي في تعطيل يمكن أن يهدد رخاء المجتمع ويقوض الأمن الوطني، والتركيز هنا، على مدى اعتمادية شبكات المعلومات، التي تساند البنية التحتية في أي بلد، والتي تساند دول العالم أجمع. ويهدف هذا الجزء من الكتاب لتبني مفهوم مشترك لطبيعة التحديات التي تواجه اعتمادية الشبكات وتحديد أساليب مكافحتها وتحييدها بين المعنيين بالتطوير التقني (من فنيين وعلماء ومهندسين) والهيئات المسؤولة عن وضع السياسات مثل وزارة الاتصالات والتقنية، وهيئة الاتصالات والتقنية، ومدينة الملك عبد العزيز للعلوم والتقنية والجامعات. وللوصول لهذه النتيجة من الضروري طرح سؤالين: أولاً: ما مدى اعتمادية شبكات المعلومات المساندة للبنية التحتية الحساسة؟ لأن فهم المشكلة من منظور تقني وإدراك بقدر مناسب للتهديدات والثغرات الأمنية، أمر ضروري وأساسي

لضمان تحديد الأولويات ومواجهتها.

وثانياً: كيف يمكن أن يطمئن المجتمع إلى أن شبكات معلومات البنية التحتية تحظى باعتمادية كافية لضمان عدم توقفها وخروجها من الخدمة؟ فتحقيق إجماع تام لتحديد المستوى المقبول من الاعتمادية يعد تحدياً مستمراً ودائماً طالما أن هناك زيادة مطردة في المكننة والأتمتة. وسيتم طرح نموذج لمحاولة الإجابة عن هذه الأسئلة في الصفحات القادمة. ورغم أن التركيز ينصب على القضايا الفنية؛ إلا أن التقنية بمفردها لا يمكن أن تكون كافية لمواجهة تحديات الاعتمادية. فالمواجهة المكتملة لابد أن تشمل إجراءات تشغيلية وتدريب ووعي وممارسات فردية وتنظيم، كعناصر ضرورية للتزامن مع التقنية. وحقيقة الأمر أن الحلول التقنية المتوافرة لا تطبق دائماً بكفاءة مجدية، بالإضافة إلى أن الإطار المتعلق بدراسة مستوى الاعتمادية، كتحدٍ للسِّياسة العامة، مطلب أولي للتصور الدقيق للمسألة والوصول لإجماع لفهم المشاكل ونطاق الحلول المناسبة.

ولكن السؤال الذي يظل قائماً هو: ما هي مكونات وعناصر البنية التحتية، التي يسعى المجتمع لمعرفة مدى اعتماديتها ومقاومتها للفشل العام؛ سواءً الفشل الناتج من الأعطال التقنية والقضاء والقدر، أو تلك الناتجة عن التخريب والإرهاب؟ ويمكن القول أن البنية التحتية في العالم تعتمد على قطاعات المواصلات والنقل وقطاعات المال والاقتصاد والطاقة والاتصالات التي أصبحت بدورها تعتمد بصورة متزايدة على المكننة الذاتية والأتمتة أو التحكم الآلي الحاسوبي. ومع تزايد تطور ونمو تقنية المعلومات، التي فتحت الباب على مصراعيه لإمكانيات جديدة أسهمت في رفع مستوى تقديم الخدمات، وخفض التكاليف ورفع الكفاءة؛ فقد نشأت أتمتة البنية التحتية وتطورت بسبب الفوائد الاقتصادية والأداء المتميز والواضح، ونتيجة لذلك تحول العالم إلى مجتمع مترابط سلكياً ولاسلكياً متجهاً نحو تعقيدات اجتماعية وثقافية واقتصادية يصعب متابعتها وفهمها. وقد نتج عن التطبيقات الواسعة لتقنية المعلومات تحديات جديدة، فيما كان ينظر إليه تاريخياً على أنه بنية تحتية صلبة ودائمة.

وتتميز التغييرات، التي طرأت على بيئة تقديم الخدمات العامة، بخفض ملموس في سيطرة التنظيم الحكومي وخفض حجم موظفي وعمال الشركات بسبب اعتمادها على التحكم التقني ومكننة العمل والتشغيل وسرعة تنفيذ الأعمال واتساع التنافسية، والانفتاح الجديد

الواسع والشامل على الأسواق العالمية، مما أدى إلى الحاجة الماسة لضمان عمل الشبكات العالمية بكفاءة وموثوقية عاليتين. وكان من البديهي أن تطرح تساؤلات كثيرة بسبب ظهور التطبيقات اللامحدودة لتقنية الحواسيب، التي تتحكم في أنظمة البنية التحتية، حول مدى الاعتماد على الأنظمة المعقدة والثغرات الأمنية، التي قد يستفيد منها القراصنة والمتسللون أو المخربون. وعلى أية حال؛ فإن العالم عليه الانتظار لمعرفة ما إذا كان المجتمع الدولي بقواه الحكومية وقطاعه الخاص ونجاحاته التقنية الرائعة والمعقدة سيستمر في تقديم خدماته المتقدمة الآلية، باعتمادية مقبولة من عدمه؛ فأهمية الخدمات التي تقدمها البنية التحتية في العالم يجعل الاهتمام باعتمادية شبكات المعلومات في أوج الأهمية وغاية الضرورة.

وتنبع تحديات الاعتمادية من مصدرين أساسين، مصدر طبيعي، ومصدر بشري. ويمكن القول إن أشد وأكبر الأعطال، التي تسببت في تعطيل الخدمات المتعلقة بالبنية التحتية، كانت نتيجة لكوارث طبيعية، وحوادث متعلقة بأخطاء في التصاميم أو التشغيل سببها العنصر البشري[٢٤]. ومن المؤكد أن البنية التحتية ستتعرض دائماً لهذا النوع من الأعطال. ورغم النقص الكبير في المعلومات والدراسات المتعلقة بالكوارث الطبيعية، وخاصة في مجال انقطاع شبكات الكهرباء في المملكة العربية السعودية، وعدم توافر التحاليل التي توضح الأسباب التقنية الحقيقية لانقطاع الخدمات الكهربائية والحلول لتلافيها؛ إلا أن الصحف المحلية ووكالات الأنباء كثيراً ما تنشر تلك الأخبار مقرونة بتكهنات عن أسبابها، وخاصة أعطال الصيف عندما تصل درجات الحرارة إلى أعلى معدلاتها.

وكثيراً ما تعزو الصحف أسباب الانقطاع إلى زيادة الأحمال وبالتالي انقطاع التيار، وما يتبع ذلك من معاناة خاصة في المستشفيات وقصور الأفراح وغيرها من المواقع الحيوية. ومعظم هذه الأعطال تصنف على أنها أعطال تسلسلية، وعلى سبيل المثال لهذا النوع من الأعطال، ما حصل من انقطاع للكهرباء في مقاطعة ينبع في يوليو ٢٠٠٧[٢٥] بسبب تأثير الرطوبة على أسلاك الضغط العالي ومحولات الكهرباء حسب ما صرح به المسئولين في الجهة المعنية. وقد أثرت تلك الانقطاعات على الأعمال والإدارات الحكومية ومنازل المواطنين، وهي مشكلة تتكرر في كل صيف، وفي الدمام والخبر تكررت الانقطاعات الكهربائية، وكذلك الحال في منطقة القصيم إذ تكرر انقطاع الكهرباء في مركز الأحمدية جنوبي القصيم، وحي الروضة في محافظة عنيزة. وفي حائل تتعالى الشكوى من انقطاع التيار في الأحياء الجديدة بالقطاعين

الشمالي والجنوبي وأحياء جنوب الدائري؛ خاصة أحياء النخيل والصفاء والنماصي والحصان والعترس والنقرة النموذجي والكعيك الحمراء والرياض الخلف واليرموك والشفاء وغيرها. وفي جازان تتأثر الكهرباء كثيراً بموجة الغبار، التي تبدأ مع فصل الصيف، وتستمر إلى ما يقارب الشهرين وتعقبها أمطار وعواصف، ملحقة أكبر الضرر بالشبكة فيما تبرز معاناة الأهالي في المراكز الصحية والمنازل والمحال التجارية، التي تتأثر بانقطاع التيار.

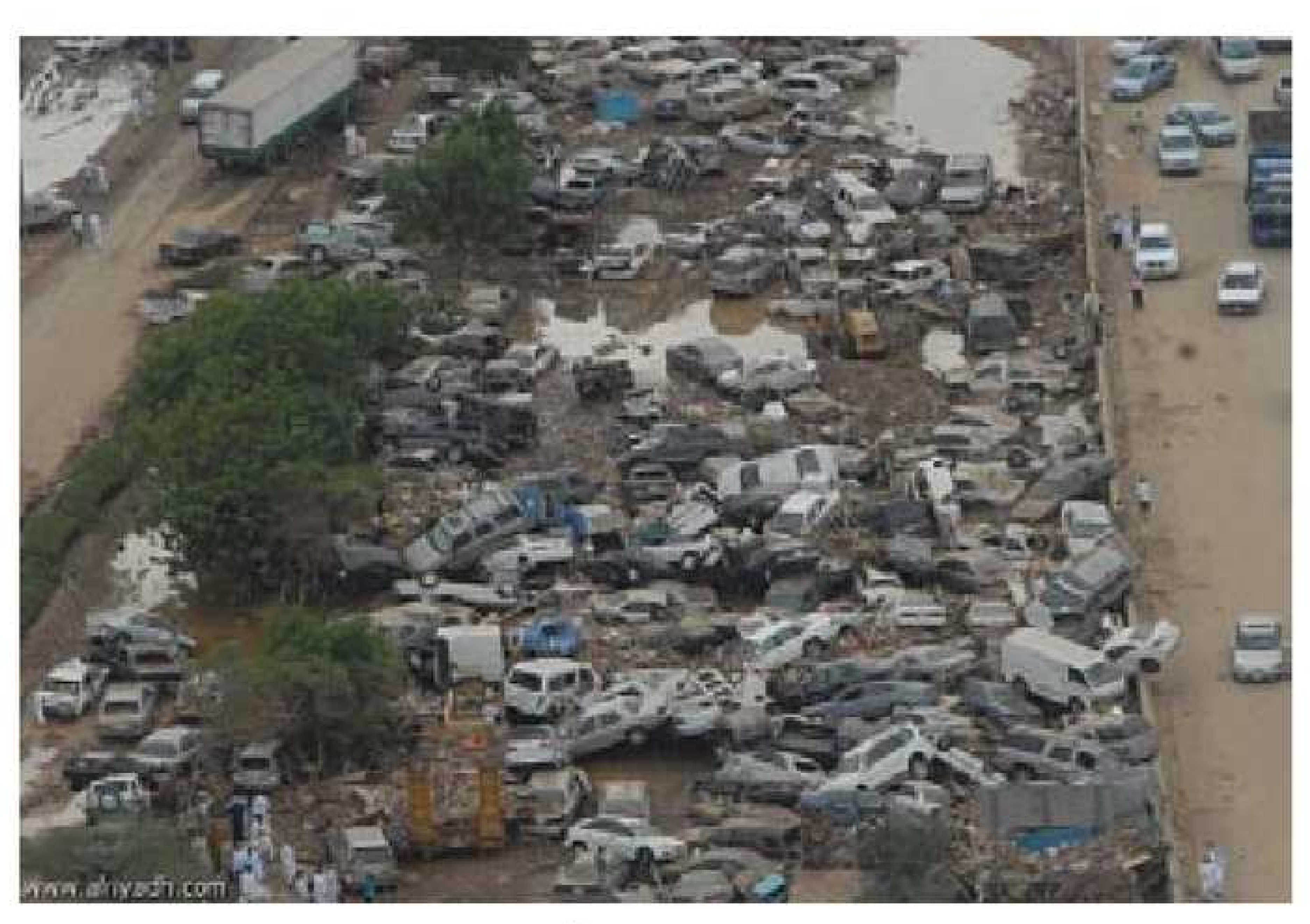
وهكذا تبدو الصورة في معظم مناطق المملكة رغم تطمينات وزارة المياه والكهرباء بأن الوزارة، ممثلة في الشركة السعودية للكهرباء، قد أنهت استعداداتها منذ وقت مبكر لاستقبال فصل الصيف بدون انقطاع، وأن الوزارة قد عَمِدَت إلى توفير فائض في الطاقة الكهربائية لكون الشركة لديها الاستعدادات الكافية لمواجهة أي طارئ. وفي هذا السياق تؤكد الوزارة أن الانقطاعات تنتج بسبب نقص الطاقة، وإذا ما حدث عطل في أي محوّل أو انقطاع في الكوابل فيتم إصلاحه في الحين. كما توضح الشركة أنه إذا ما حدث انقطاع للتيار في أي منطقة، فيكون نظراً لتعرض بعض المناطق الأخرى، وخاصة المدن الكبرى مثل الرياض وجدة المرتبطة بها للأعطال المفاجئة فتستعين تلك المناطق بمولدات من بقية الشبكة بصورة تلقائية. ومن المؤكد أن يتسبب ذلك في رفع أحمال تلك المناطق مما قد يتسبب في عطلها وتستعين هي الأخرى بمناطق متصلة معها، وهكذا الأمر الذي قد يؤدي، لا قدَّر الله، إلى فشل تسلسلي شامل.

أما فيما يتعلق بالأعطال المتعمدة بواسطة ناشطين عدائيين؛ فإنها في تزايد مستمر على مستوى العالم، بسبب تزايد نشاط قراصنة الحواسيب، نتيجة لتزايد أعدادهم وتزايد قدراتهم وأدواتهم الفنية من ناحية، وبسبب تزايد التهديدات الإرهابية من ناحية أخرى. وهذا يعني أن الاهتمام بهذين التهديدين المزدوجين، بأسلوب مدروس ومتزن، يجب أن يعطى أولوية طويلة الأمد في السياسات العامة لأي بلد في العالم. وتواجه اعتمادية الشبكات مشاكل فنية ومخاطر متعددة، ومن الضروري وضع اليد على جميع أنواع ومسببات هذه المخاطر وشرحها وتحديد المسار المقترح لمعالجتها وتلافيها، بالإضافة إلى تصنيف الإخفاقات والقصور ووضع الأطر والمفاهيم التي تصنفها في سياق قوائم فنية محددة. وينبغي أن تتمثل تلك المواجهة في تطوير فهم وإدراك تحليلي للاعتمادية الموجودة والثغرات الأمنية وبيئة التهديدات وإنشاء نظام إجرائي هندسي يتعامل مع التهديدات كعنصر أساسي في النظام يعالج موضوع الاعتمادية ويصنفها ضمن تلك العناصر الأساسية في المنظومة الشبكية، ووضع الأسس التي تكفل

مواصلة الالتزام والحذر واليقظة والتدريب المستمر لكامل المجتمع بهدف تعزيز الاعتمادية وتقويتها.

التصنيف العام لإخفاقات البنية التحتية

تصنف الإخفاقات حسب أسبابها والأدوات التي استخدمت لإحداثها. وتتدرج المسببات من ظواهر طبيعية صرفة، كالتي تنتج بسبب الطقس والكوارث الطبيعية والقضاء والقدر، إلى الأعمال التخريبية المتعمدة من قبل أشخاص يتعمدون إحداث الضرر. وبين هذين السببين المختلفين يقع مجال واسع من الحوادث أو العوارض غير المتعمدة بدرجات مختلفة من



شكل (٦): طريق الحرمين أثناء الكارثة

التدخلات والحوافز البشرية. وبالمثل؛ فإن الآليات التي تؤدي إلى الإخفاق تتنوع بين فئتين متباعدتين، إحداهما تتسبب في فشل محلي يتحول إلى فشل شامل من خلال سلسلة متتالية من ردود الفعل، التي تؤدي إلى فشل في نظام جزئي أو عنصر من عناصر النظام يتوالد بصورة مطردة في بقية أجزاء الشبكة، حتى يختل النظام أو ينخفض مستوى أدائه بصورة مؤثرة،

والأخرى قد تكون بتخريب شامل لموقع مهم في الشبكة يؤدي للنتيجة نفسها.

وقد يكون من الأجدى النظر في الأمثلة والأسباب التي أدت إلى حدوث الفشل الشامل لشبكات الطاقة الكهربائية في الولايات المتحدة الأمريكية، وهي مستنبطة من دراسات أمريكية موثوقة، مثل التقارير التي تصدر من مكتب الحكومة الأمريكية لمتابعة الاعتمادية United States Government Accountability Office (GAO)، والتقارير الخاصة الموجهة لرئيس الولايات المتحدة المتعلقة بموضوع الكوارث والبنية التحتية[٢٦]. ويرجع سبب اللجوء للحالات الأمريكية إلى شح التقارير الفنية الدقيقة، التي توضح الأسباب الحقيقية لانقطاع الكهرباء في بعض مناطق المملكة العربية السعودية والدول العربية، والاكتفاء بتفسير الوضع بأنه نتيجة زيادة الأحمال كما ذكر سابقاً.

ومن أبرز تلك الكوارث على سبيل المثال؛ الفشل الشامل الذي حصل في منطقة واسعة في غرب الولايات المتحدة الأمريكية في صيف عام ١٩٩٦، بسبب عطل يسير في خط من خطوط نقل الكهرباء في ولاية أوريجان «Oregon» نتج عنه ردود فعل في نظام نقل أوامر التحكم، أدت إلى تعطيل بعض المولدات في عدة ولايات، وإخراجها من الخدمة، ثم توالى إخراج المولدات بأسلوب تتابعي، حتى أظلمت معظم ولايات الجزء الغربي من أمريكا. وتشير الدراسة إلى أنه يمكن حدوث خلل شامل دون أن يكون نتيجة أعطال تتابعيه، وإنما بسبب توقف نظام فرعي أساسي، ومن أمثلة ذلك الأعطال الشاملة، التي حصلت في كهرباء نورثردج «Northridge» نتيجة لزلزال كاليفورنيا عام ١٩٩٤م، الذي تسبب في انقطاع الكهرباء وخدمات الهاتف عن ملايين المشتركين، وكان بسبب عطل في الشبكة، ولم يكن بسبب أعطال تتابعيه. فالمثال الأول يشبه تأثير الدومينو، التي تسقط بالتتالي عند سقوط القطعة الأولى بينما المثال الآخر يشبه سقوط جميع القطع عند هز الطاولة.

إن كثيراً من التهديدات المكتشفة والمعروفة عالمياً، التي تهدد شبكات المعلومات المساندة للبنية التحتية الوطنية في المملكة العربية السعودية لم تجرب فعلياً حتى الآن، لأن المملكة العربية السعودية لم تتعرض ولله الحمد لمثل هذه الأعطال الشاملة باستثناء كارثة جدة في آخر عام ٢٠٠٩م[٢٧]، التي بلغ عدد الوفيات فيها إلى ١٢١ حالة، وعدد بلاغات الحالات المفقودة ٣٩ حالة، وبلغ عدد العقارات المتضررة ١١٩٣٥ عقاراً، بينما وصل عدد المركبات المتضررة

١٠٩٩٩ مركبة، وذلك حسب ما أعلنته لجنة تقصي الحقائق المكلفة بموجب أمر ملكي وما تناقلته جميع وسائل الإعلام المحلية الصادرة في ذلك التاريخ. وكان الفساد الإداري سبباً أساسياً لتفاقمها، حيث اكتشف المواطنون والمسؤولون أن معظم البنية التحتية المتعلقة بتصريف الأمطار والسيول لم تنفذ رغم قيام الدولة برصد بلايين الريالات وصرفها على تلك المشاريع. كما أن مجاري السيول وأوديتها قد بيعت كمخططات سكنية وحصل مالكوها على تصاريح من الجهات المختصة بصلاحيتها للسكن وحمايتها من انغلاق مجاري السيول وسد منافذها وعدم وجود ما يؤدي إلى منع بناء المساكن فيها.

ولا شك أن عدم خوض المملكة في هذه التجارب الكوارثية يجعل التنبؤ وأخذ الحيطة لمنع التهديدات أكثر صعوبة لعدم توافر التجارب اللازمة لذلك. لذا فقد تكون أو ل خطوة لتحسين اعتمادية الشبكات بصورة عامة، هي التعرف على مستوى الاعتمادية والثغرات الموجودة في تلك الشبكات وتحديد بيئتها وأنواعها، وهذا يتطلب تشكيل لجان متخصصة ومتفرغة لإجراء فحوصات واختبارات مفصلة لهيكلية الشبكة، وإجراء دراسات شاملة لمخططاتها وتصميماتها الهندسية ومعداتها وبرامجها وروابط اتصالاتها، وتقييم مكوناتها البشرية ومكونات سياسات التشغيل بهدف استخدامها كدليل يسترشد به لبناء إجراءات هندسية لتحقيق مستوى عالٍ للاعتمادية. ولا يمكن تحقيق مثل هذه المستويات العالية للاعتمادية دون اعتبارها عنصر مقايضة أساسي في عملية الإجراءات الهندسية الشاملة، لأن المستوى المقبول للاعتمادية يقابله تضحيات في إمكانيات الشبكة ومستوى خدماتها. لهذا فإنه يتوجب قبل اتخاذ أي قرار يؤدي إلى تغيير بنية الشبكة إجراء دراسة مستفيضة لتحديد الفوائد والمميزات التي ستفقد بسبب هذا التغيير. وكثيراً ما يؤدي تطبيق استراتيجية جديدة لمنع تهديدات معينة إلى نشوء ثغرات أمنية جديدة في مكان آخر من الشبكة، كما ينبغي الأخذ بالاعتبار أن مقدار تأثير مشكلة معينة ونسبة حصولها قد لا يبرر تكاليف الحلول المقترحة؛ بالإضافة إلى أنه من الضروري معرفة التكاليف بدقة وتوضيح، وتفهم ما يؤول إليه أداء الشبكة عند تطبيق أي استراتيجية جديدة. ومن أهم الإجراءات الواجب اتباعها، تصميم منهجية لموازنة المقايضات في عناصر عمل الشبكة، التي لا يمكن تلافيها مع العوامل الأساسية، مثل الأداء والتكلفة والاعتمادية، ويدخل في إطار القائمة الفنية ـ أيضاً ـ مراعاة الالتزام باليقظة والحرص الشديد، والتعليم التثقيفي، المستمر وعقد الندوات والورش الفنية

الموجهة لرفع الوعي التام بمشاكل الاعتمادية في المجتمع بجميع مكوناته وفئاته ومؤسساته الرسمية والمدنية.

ومع تزايد النمو الكبير في شبكات المعلومات المتعلقة بالبنية التحتية في الحجم والتعقيدات، نشأت حاجة عاجلة لتنظيم وسائل وطرق لإدراك وتطبيق الدروس المستفادة من مشاكل الإخفاق والقصور في أي جزء من الشبكة، وهذا بدوره أدى إلى ضرورة تطوير أدوات وإجراءات وآليات لاكتشاف التهديدات والأعطال، وتصميم وسائل وأساليب لرصدها والتبليغ عنها، وتحديد واضح لتسلسل ردود الفعل الواجب اتباعها، وتحديد الجهات والإدارات الواجب إبلاغها وواجبات كل جهة. كما تتطلب خطة تحسين اعتمادية الشبكات إلى اعتماد أطر ووسائل تنظيمية غير متحيزة في حدود تشريعية واضحة لتدفق المعلومات الاستخباراتية المتعلقة بالثغرات والتهديدات والأعطال في وقت واحد لجميع المعنيين بالبنية التحتية، سواءً الرسمية منها أو الخاصة، وعلى وجه التحديد إدارات الخدمات العامة ومرافقها المسؤولة عن حماية بيانات الأعمال الحساسة، وكذلك المسؤولون عن المرافق والطرق والاتصالات، حيث سيكون لذلك أثر كبير في توضيح بيئة التهديدات، كما أنه يحقق استجابة مؤثرة لمعالجة أي طارئ. ورغم أن المستفيد الأول من رفع مستوى الاعتمادية في البنية التحتية هو القطاع الخاص، الذي لابد له من تفهم موقعه المهم لضمان اعتمادية البنية التحتية وتطويرها؛ إلا أنه لا يمكن تجاهل دور الحكومات وواجبها لأخذ المبادرة في هذا المجال. ويمكن القول أنه لابد من تضافر الجهود الحكومية وجهود القطاع الخاص لرفع مستوى الاعتمادية، لأن أي منهما لا يستطيع تحقيقها منفرداً، والمصلحة الوطنية العامة لا يمكن تحقيقها واستدامتها دون التعاون المشترك بين الدولة والقطاع الخاص والمجتمع بجميع فئاته ومستوياته.

المخاطر التي تعترض البنية التحتية

إن اعتبار البنية التحتية نقطة ضعف مميتة للدول الحديثة ليس من باب المبالغة[٢٨]، والواضح الجلي أن الإرهابيين قد تعلموا استراتيجيات وطرق فعالة لمحاربة الدول النظامية بهدف إلحاق خسائر اقتصادية كبيرة للدول المستهدفة. وفي هذا الإطار لا يمكن أن ننسى تصريح زعيم القاعدة «أسامة بن لادن» لشبكة «سي. إن. إن» الأمريكية، عندما قال قبل كارثة

١١/٩ «سنعمل على ضرب مفاصل الاقتصاد الأمريكي». ولا يخفى على أحد أن شبكات البنية التحتية تشكل أساس الثروات والوظائف والأعمال اليومية، ومع ذلك فهي غير حصينة ومعرضة للهجوم والاختراقات المؤثرة.

ومع أن محاولة تفجير «الحلقات الحرجة» في البنية التحتية، التي هي أهم حلقة في النظام، والتي تتعامل مع معظم أوامر الشبكة وتتحكم في تشغيلها وتوزيع الأحمال ـ والتي يمكن أن تشل كامل الشبكة المستهدفة عند تخريبها ـ ليست جديدة، إلا أنه بدأ ينحو منحىً جديداً، حيث وجد بيئة تجعله في صدر الأعمال الإرهابية، لقناعة الإرهابيين بأن شبكات نقل الطاقة الكهربائية والاتصالات، تمثل هذه الأيام جزءاً مهماً وحرجاً للغاية في حياة المجتمعات، فهي تمدها بكل احتياجات المعيشة الضرورية، وسيعيش أي مجتمع في ضياع تام بدون هذه الشبكات. وللمتابع أن يتخيل المجتمع الذي يعيش فيه قد تحول بين لحظة وضحاها إلى مجتمع يعيش دون شبكات اتصالات، ودون شبكات الطاقة الكهربائية، ودون غاز وماء. فمجتمع مثل هذا سيعود لاستخدام الدواب للنقل، وسوف يتعطل لدية النظام المصرفي والمالي، وباختصار؛ فإنه سيعيش في عصور ما قبل الثورة الصناعية. ولا يكفي مجرد التفجير العشوائي، أن يكون سبباً للتخريب الشامل للشبكات، لأن معظم شبكات البنية التحتية مهيأة لمقاومة الأضرار العشوائية؛ لكن المخيف هو أن معظم مكونات البنية التحتية لم تصمم لمقاومة الإرهاب، لأن معظم الشبكات أنشئت قبل ظهور بيئة الإرهاب كما نعرفها اليوم، وإنما كان الهدف في الماضي هو مقاومة الكوارث الطبيعية أو العيوب الناتجة من التصاميم الهندسية والإنشائية. وتتركز المقاومة في الغالب على تطبيق بوابات ومداخل إلكترونية حصينة لمنع الدخول غير المشروع، أو من خلال المنشآت التبادلية، أي إحلال منشأة محل أخرى متعطلة لضمان استمرار الخدمات.

ولتنفيذ عمل إرهابي مؤثر، يلجأ منظمو الإرهاب إلى تجنيد عدد كبير من المتخصصين الملمين بقدر كبير من علوم الشبكات، وتكليفهم بجمع معلومات ميدانية دقيقة ومحددة لمواقع الحلقات الحرجة في الشبكة المستهدفة، وهذا ما بدأ يتكشف في الولايات المتحدة الأمريكية، إذ إن الجهات الأمنية قبضت مؤخراً على خلية إرهابية لجمع المعلومات عن حلقات الشبكات الحرجة. وفي مارس عام ٢٠١٠م نشرت كثير من الصحف خبر القبض على الأمريكي «شريف موبلي» من «نيوجيرسي»[٢٩]، وهو واحد من ١١ من المتهمين بالانتماء إلى تنظيم القاعدة في

اليمن الذين تم القبض عليهم، ووصفته بالرجل النووي، حيث سبق له العمل في ثلاثة من المفاعلات الأمريكية في الفترة ما بين عامي ٢٠٠٢ و٢٠٠٨م. وكان من المهام الموكلة إلى موبلي القيام بأعمال الصيانة ونقل مواد مختلفة، غير أنه سافر إلى اليمن، وهو ما أثار مخاوف عديدة في الأوساط الأمريكية من إمكانية تسريبه لمعلومات نووية للقاعدة.

كما يمكن، في حدود ضيقة، تحديد الحلقات الحرجة، إما بالدراسة الأكاديمية أو عن طريق المحاولة والخطأ، وبالإمكان شل شبكات البنية التحتية بشمولية مخيفة وسهولة مزعجة، عن طريق اختيار الحلقة الحرجة في الشبكة، ولكن مجرد معرفة وفهم علوم الشبكات ليس كافياً، فالهجوم الناجع يتطلب معرفة دقيقة ومحددة للحلقة الحرجة، التي تمثل «الحلقة القاتلة» في الشبكة المستهدفة، ولتحقيق شلل كامل لأي شبكة؛ فإن الإرهاب الدولي يتجه إلى تسديد هجماته لتلك الحلقات.

ولا يستغرب أن تتركز جهود الجيل القادم من الإرهاب الدولي على محاولات حثيثة لتدمير ما يستطيعون تدميره من البنية التحتية العالمية. ويمكن القول أن تعطيل أو عزل عدد قليل من الحلقات والنقاط العادية يمكن أن يتسبب في تعطل أي شبكة، وذلك بسبب تقسيمها إلى جزر معزولة عن بعضها. إلا أن كثيراً من المحللين المتخصصين في الشبكات الديناميكية يؤكدون وجود طرق أسهل لتدمير شبكات البنية التحتية، في إشارة إلى الأعطال التسلسلية المتتالية[٣٠]؛ لأن شبكات البنية التحتية ليست ساكنة بل «ديناميكية» وتتدفق من خلالها المعلومات والبيانات والطاقة والمواد بصورة دائمة ومنتظمة، وهذه الديناميكية تؤدي إلى نشوء مجموعة جديدة من الثغرات الأمنية، التي يمكن استغلالها من قبل المنظمات الإرهابية العالمية. وتحصل الأعطال التسلسلية في الشبكات الديناميكية، حتى لو كان العطل في نهاية طرفية منفردة إذا كان يتعامل مع أحمال عالية، لأن الأحمال التي تتعامل معها كل طرفية في الشبكة يتم توزيعها ديناميكياً في معظم شبكات البنية التحتية، وعندما تتعطل أو تعزل نهاية طرفية، نتيجة لحادث عرضي أو هجوم متعمد؛ فإنه يتم إعادة توزيع الأحمال التي تتعامل معها تلك الطرفية بسرعة على بقية النهايات الطرفية في الشبكة. وتؤدي إعادة توزيع الأحمال على بقية أجزاء الشبكة إلى زيادة كبيرة في تدفق المعلومات ينتج عنه إغراق النهايات الطرفية الأخرى، التي لا تتمتع بقدرات عالية.

ولحماية مثل هذه الطرفيات النهائية في الشبكة؛ فإن معظم الأنظمة تخرج النهاية الطرفية المحملة بأكثر مما صممت له بصورة تلقائية من الشبكة وتعيد توزيع أحمالها على بقية محطات الشبكة، مما ينتج عنه أعطال متتابعة في بقية الأجزاء حتى تصل إلى توقف تام وشامل، لأن كل عطل في المحطة يؤدي إلى توزيع أحمال تلك المحطة على بقية أجزاء الشبكة. ومثل هذه الأعطال التسلسلية لا تحدث إلا في الشبكات غير المتجانسة، وهي التي لا يكون توزيع الأحمال بين نهاياتها الطرفية متساوياً، لكنها تتألف من نهايات طرفية قليلة بسعات أحمال عالية وبقية النهايات تكون ذات سعات منخفضة. أما الشبكات المتجانسة، التي تكون الأحمال في جميع مكوناتها متساوية؛ فإنها لا تعاني من الفشل التسلسلي إلا في أحوال خاصة، وذلك عندما تتوقف أكثر من محطة في آن واحد ويكون في الغالب بفعل إرهابي مخطط له، ولكن لسوء الحظ؛ فإن جميع شبكات البنية التحتية غير متجانسة بسبب متطلبات التصاميم.

كيف يفكر ويخطط الإرهاب العالمي؟

معظم الإرهابيين ليسوا عبثيين، بل أنهم برمجوا أنفسهم للاعتقاد أن العالم سيكون أفضل من خلال إرهابهم وقتلهم للأبرياء، ويبررون أعمالهم الإجرامية بالحالة المزعجة التي وصلت إليها بلدانهم، وهم مقتنعون أن المخرج الوحيد هو الصدام والصراع والجهاد، ولم يغفلوا عن الاختلال الحاد في موازين القوى بين الأمم، التي ينتمون إليها والعالم الغربي لغير صالحهم، ولكنهم يرون أن سد الفجوة في هذا الاختلال يمكن تعويضه بالتضحية بالنفس وإيقاد نار الجهاد وتغذيتها وفتح الجبهات في جميع بقاع الأرض. كما أنهم ينظرون إلى الصلح مع الأعداء على أنه خيانة واستسلام.

والسؤال المهم: كيف نشأ الإرهاب؟ ولمحاولة الإجابة ننظر للقاعدة كونها أصبحت رمز الإرهاب العالمي، وما من شك أن القاعدة ولدت من رحم الجهاد الأفغاني، أما والدها فهو المخابرات المركزية الأمريكية، التي دعمت ودربت وسلحت المجاهدين لدحر الاحتلال الروسي، ولم تستفد المخابرات الأمريكية من تجربة فيتنام، التي أثبتت أن المعتقدات خط أحمر لا يمكن التلاعب بها. ومن المعلوم أنه عند تهيئة أي فرد للدفاع عن عقيدته؛ فإنه من الصعب، بل قد يكون من المستحيل إعادته لوضعه السابق، لأنه قد جرت برمجته ليعتقد أنه يحارب حربه

وليس حرب من جنده، لذلك؛ فإنه لن يترك سلاحه، حتى يحقق ما جاء من أجله ولو كان ذلك مستحيلاً. إن أمريكا هي من دفعت صغار السن من الشباب للجهاد بحجة الدفاع عن إسلامهم ضد الشيوعية الملحدة، وهي التي فتحت مراكز التدريب وعلمتهم كيف يصنعون القنابل من موادها الأولية، وكيف يحاربون في المدن وزودتهم بكم هائل من الأسلحة، التي لازالت لدى القاعدة حتى اليوم.

ويعد الحديث عن الإرهاب وتحليله ومعرفة ما يدور في عقول وأذهان الإرهابيين أمراً ملحاً يجب تداوله على أصعدة متعددة، وقد تناولته هيئات شتى من خبراء الإرهاب والجامعات المتخصصة ووسائل الإعلام لتشكيل وصف دقيق للإرهاب، بهدف الوصول إلى معرفة واضحة بحقيقته. ومن الضروري الدخول إلى عقول الإرهابيين وتسجيل ما يدور بخلدهم وتحديد أساليب وطرق التجنيد الجديدة التي يتبعونها، وخاصة أساليب الذين يتَّخذون من «أسامة بن لادن» قدوة لهم. وباعتبار أنَّ شبكة الإنترنت قد تحوَّلت إلى أداة مركزية، من الممكن أن تُغني حتى عن معسكرات التدريب، التي كانت موجودة سابقًا في أفغانستان وتجعلها غير ضرورية، ولم يعد سراً معرفة الأساليب، التي تتبعها تلك التنظيمات باستخدام متقن لتقنية الإنترنت، يتم من خلالها إيصال دعوة بريئة لاعتناق الإسلام لمن لا يدين به في الغرب، أو قبول المبادئ التي يحارب من أجلها التنظيم. وهذه الدعوة في الظاهر مرحلة بعيدة كل البعد عن الإرهاب، ويؤيدها الجميع، ومن الصعب محاربتها قانونياً. ثم تأتي بعدها مراحل متدرِّجة بحيث يكتشف فيها الفرد المستهدف المبادئ السياسية المتطرِّفة، ويتخذ موقعاً لنفسه ضمن المجتمع العالمي الذي ينتهج التطرف. عندئذ تأتي المرحلة التالية، وهي مرحلة التلقين المباشر، وتبادل الآراء والأفكار، وتوضيح الظلم، الذي تعاني منه الشعوب التي تنتمي لها تلك المنظمات في شتى أنحاء العالم والتجاوزات غير الإنسانية، التي تمارسها أمريكا والدعم اللامحدود للكيان الصهيوني، الذي يمارس قتل الأطفال والنساء وهدم منازلهم. وتطعَّم هذه المعلومات بالصور والمقاطع الحية، التي تؤكد ما يجري على أرض الواقع، مما يبعث روح الحماس والرغبة لإيقاف مثل هذا العنف الجائر الذي تستخدم فيه أموال دافعي الضرائب الأمريكية ومعداتها الحربية، مثل طائرات الأباتشي والقنابل العنقودية والأسلحة المحرمة دولياً وتطعم هذه الصور بأخرى من الممارسات، مثلما يحدث في السجون السرية الأمريكية من فضائح، كما حصل في «أبو غريب» وغيره، وفي نظر قادة ومنظري الإرهاب يعد دافعي الضرائب ممولين

لكل ما تقترفه بلادهم من قتل وتدمير، وبهذا يبررون لأتباعهم قتل الأبرياء في أي مكان.

وفي مقابلة أجراها ديفيد بار ساميان مع إدوارد سعيد ونشرت في كتاب «الثقافة والمقاومة»[٣١] في العام ٢٠٠٣م، تحدث إدوارد سعيد بإسهاب عن «أصول الإرهاب، وقال: «أعتقد بأن الحادثة (٩/ ١١) جاءت في أعقاب جدل طويل حيال تورّط الولايات المتحدة في الخارج، الذي امتد عبر القرن الماضي برمّته. وشمل ذلك التدخل في شؤون العالم الإسلامي والدول المنتجة للبترول والعالم العربي والشرق الأوسط، وكلّ تلك المناطق التي تعد أساسية لصيانة المصالح والأمن الأميركيين، تلك المصالح التي تضمّ البترول والقوة الاستراتيجية معاً... أعتقد بأن معظم العرب والمسلمين يشعرون بأن الولايات المتحدة لم تبد في الحقيقة أي اهتمام برغباتهم، وإنما دأبت على ممارسة السياسات التي تخدم إسرائيل، حتى ولو تعارضت مع مصالح أمريكا نفسها، دون أن تبذل أثناء ذلك أية محاولة لتبرير تلك السياسات بشكل ما أو لتوضيح ماهيتها، وهي (أي أمريكا) فوق كلّ شيء، تواصل انتهاج هذه السياسات دون العودة إلى أي من المبادئ، التي تزعم الولايات المتحدة بأنها حكر عليها وحدها مثل: الديمقراطية، وتقرير المصير، وحرية التعبير، وحرية التجمّع والالتزام بالقانون الدولي. إن تبرير احتلال الضفة الغربية وغزة مثلاً، الذي مضى عليه أربعة وثلاثون عاماً هو أمر في غاية الصعوبة، وكذلك وجود المئة والأربعين مستوطنة وما يقدر بأربع مئة ألف مستوطن تم جلبهم بدعم وتمويل من الولايات المتحدة، بحيث نقول بعد ذلك إن هذا يمثل جزءاً من التزام الولايات المتحدة بالقانون الدولي وقرارات الأمم المتحدة. وبمجرد القناعة بما يقوله إدوارد سعيد، وهو يمثل واقع الحال، يبدأ الشخص الذي يتابع التجنيد بالتيقن من تجاوب وتعاطف المتلقي، ويكون العميل الإرهابي قد كون فكرة واضحة عن نفسيته ومعرفة مدى استعداده للمشاركة في وقف الظلم والعنف الذي يمارسه الغرب ضد دول العالم الثالث، الذي تعرِّفه القاعدة «بالمستضعفين»، وبناءً على عمر الشخص المستهدف وقدراته الذاتية واستعداداته النفسية، تأتي مرحلة توضيح الثواب، الذي ينتظر كل من يُسْهِم في رفع الظلم عن المظلومين، ومميزات الشهادة والدعوة للجهاد والعمل الجهادي. وتكمن ذروة نشر التطرّف وترسُّخه في التحوّل إلى النشاط الإرهابي، الذي يرافقه الاستعداد للموت شهيدًا وهنا يبدأ الحديث عن «نشر الجهاد» وتوضيح الثواب

العظيم، الذي ينتظر من ينجح في إضافة عنصر استشهادي جديد للمنظمة؛ وهو مفهوم يزعج الغرب بصورة عامة وأمريكا على وجه الخصوص.

أما فيما يتعلق بالمفهوم العام لاستخدام التقنية؛ فإنه يمكن متابعة الحقائق، التي رصدتها الجهات الأمنية في شتى أنحاء العالم لاستخلاص خططه بصورة متكاملة وواقعية كما يلي:

- عندما فككت السلطات البريطانية خلية من الإرهابيين المشتبه بهم في أغسطس عام ٢٠٠٤م، تسربت تقارير جرى تداولها بين البريطانيين والجهات الأمنية الأمريكية، تؤكد على أن الخلية كانت تسعى لبناء قنبلة إشعاعية قذرة، إذ كشفت عملية المراقبة المعروفة بـ«عمليات الترتر» عن العثور على كمية كبيرة من أجهزة كشف الدخان المنزلية كانت مخبأة لدى بعض أفراد الخلية، ويشتبه في أن الجماعة تريد تفكيك هذه الأجهزة لتجميع كميات كافية من مادة «الأمريسيوم ـ ٢٤١ Americium» وهي مادة مصنعة من مواد كيميائية مشعة[٣٢].

- وجد خبراء الاستخبارات الباكستانية أن جماعة «عسكر طيبة»، التي دبرت الهجمات المدمرة في مومباي، والتي أودت بحياة ١٦٦ شخصا في عام ٢٠٠٨م كانت قد اشترت ٥٠ مجموعة من الطائرات الشراعية بدون محرك، ويفترض استخدامها لتنفيذ هجوم جديد، ومن المؤكد أن توجُّه المفجرين الانتحاريين يتجسد في مهاجمة المدن المزدحمة، وتعتقد الجهات الأمنية الهندية أن مثل هذا الهجوم سيكون في الواقع صعباً للغاية، لأنه من الضروري الإقلاع من نقطة عالية، أو الاستعانة بسيارة أو زورق لسحب الطائرة الشراعية. ولكن الفكرة مخيفة للغاية على أي حال.

- تمكنت قوات الأمن السعودية في حج عام ١٤٢٩هـ من القبض على أحد أتباع القاعدة، الذي قام بمقابلة شخص قدم من خارج المملكة إلى مكة المكرمة[٣٣]، وهو يحمل ذاكرة هاتف جوال مخزن فيها رسالة من «أيمن الظواهري» تتضمن تزكية لحامل الرسالة، ليتمكن من خلالها من جمع الأموال بحجة دعم المحتاجين من الأسر في باكستان وأفغانستان، وذلك جرياً على عادتهم في تقديم دليل يطلبه المتعاونون للتثبت من انتمائهم للقاعدة. وقد تضمنت رسالة الظواهري ما نصه «إلى من تصله رسالتي هذه، السلام عليكم ورحمة الله وبركاته، وإن حامل هذه الرسالة من الإخوة الموثوقين لدينا، فبرجاء تحميله ما

تتبرعون به من أموال لمئات من أسر الأسرى، فك الله أسرهم، والشهداء رحمهم الله في باكستان وأفغانستان، والله في عون العبد ما كان العبد في عون أخيه، وآخر دعوانا أن الحمد لله رب العالمين، وصلى الله على سيدنا محمد وآله وصحبه وسلم، والسلام عليكم ورحمة الله.. أخوكم أيمن الظواهري».

- انفجار فندق فرح يوم الجمعة ١٦ مايو٢٠٠٣م في الدار البيضاء في المغرب، هو الذي كشف هوية خلايا الانتحاريين والمخططين للعمليات الانتحارية، وكان أول خيط أمسك به المحققون هو الانتحاري الناجي (محمد العمري)، حيث عثر رجال الأمن المغربي على عبوة ناسفة وبقايا مواد تستعمل في تصنيع المتفجرات والقنابل اليدوية، ثم ألقي القبض على شخص حاصل على شهادة جامعية في الفيزياء كان قد ساعد الانتحاريين في صنع المتفجرات باستعمال البارود. وهذا يؤكد معلومات أخرى كثيرة في شتى أنحاء العالم جميعها يشير إلى أن الإرهابيين يتصيدون الشباب المتخصص في شتى العلوم الحديثة.

- كشفت وثائق ومعلومات تلقاها جهاز الأمن الألماني لمكافحة الجريمة المنظمة والإرهاب من أجهزة أميركية وبريطانية[٣٤]، نشرت في ١٥ نوفمبر ٢٠٠١م، أن تنظيم القاعدة لم يكن في أفغانستان سوى دولة إرهاب قائمة بذاتها، وفق ما ورد في المعلومات الشاملة عن تفاصيل تخرُّج عدة آلاف من رعايا ٥٠ دولة، تدربوا في معسكرات القاعدة، على كل ما يرهب ويرعب من تصنيع سكين خشبية إلى السموم الكيماوية والغازات والبيولوجيات والنوويات في ١٢ معسكراً سيطرت قوات التحالف على ما بقي منها بعد تدميرها بالقصف الأميركي بحسب ما ذكره «ألريش كير وستين»، رئيس جهاز BKA الألماني للمكافحة المتنوعة على الجريمة والإرهاب في ملخص التقرير، المحذر في نهايته من صعوبة محاصرة الإرهاب إذا ما دخل مرحلة العولمة.

- في ندوة علنية عقدها رئيس جهاز مكافحة الجرائم المتنوعة السيد «كير وستين» في "فيسبادن" في نوفمبر عام ٢٠٠١م، اشترك فيها مسؤولون من أجهزة مخابراتية وأمنية ألمانية ونمساوية وبريطانية وأميركية، ومن بينهم مايكل رولينس، رئيس جهاز مكافحة الإرهاب في مكتب التحقيقات الفدرالي «إف.بي.آي»، بالإضافة إلى ديتر كأودين، رئيس جهاز BND الألماني للمكافحة، التابع بدوره للمخابرات الخارجية، وكشف في الندوة، التي نقلت وقائعها وكالات محلية للأنباء بألمانيا، أن ابن لادن اتخذ احتياطات لردود الفعل الأميركية إذا ما وجهت القاعدة ضربة، كالتي قامت بها في واشنطن ونيويورك في ٩/ ١١/ ٢٠٠١م، لذلك التحمت

منظمة ابن لادن بحركة طالبان وتكاتفتا على العمل في تطوير التدريبات بالمعسكرات، لتدخلا في مرحلة جديدة من الإرهاب الدولي، أي امتلاك أسلحة الدمار الشامل لردع ردة الفعل الأميركية حسب ما جاء في الندوة.

من هذا يمكن استنتاج أن الإرهابيين يركزون تفكيرهم حول استخدام التقنيات الحديثة، والاستعانة بالمتخصصين في مجالات علمية مثل: الفيزياء، والرياضيات، والطب، والإلكترونيات، والاتصالات، وعلوم الكهرباء. وتعد الإنترنت تقنيتهم المفضلة للتواصل، وتجنيد العناصر وخاصة صغار السن، كما أنهم يركزون الآن على استقطاب عناصر من أصول غربية. وتسعى المنظمات الإرهابية بجدية للحصول على أسلحة الدمار الشامل، إما بتصنيعها أو الحصول على بعضها جاهزاً، مما يتم سرقته من دول كانت تدور في فلك الاتحاد السوفيتي السابق، كأوكرانيا بالذات، أو من روسيا حالياً، حيث كانت المواد الخام تمر سراً عبر حدود أفغانستان مع أوزبكستان أو طجيكستان، طبقاً لما كشفته وثائق تم العثور عليها في بقايا مختبرات ملحقة بالمعسكرات، التي تم تدميرها بالطائرات من الجو، ومثل هذه الطموحات تكون في العادة طموحات دول لا منظمات إرهابية، مما جعل الوكالات الأمنية الغربية تنظر لابن لادن على أنه يمثل رئيساً لدولة قائمة بذاتها في أفغانستان، لا زعيماً لتنظيم متطرف.

اختيار ومهاجمة الثغرات الأمنية في الشبكات:

إن أهم استراتيجيات أرباب المنظمات الإرهابية يكمن في حرصهم على تحقيق عدة أهداف تعد في نظرهم أهدافاً استراتيجية؛ منها إلحاق خسائر مادية كبيرة لزعزعة الاقتصاد المستهدف، والمؤكد أن نسبة الفائدة بين خسائر المنظمات الإرهابية والدول المستهدفة ليست في صالح المجتمع الدولي. فعند مهاجمة أي نظام وتعطيله تصبح نسبة عوائد الربح في مصلحة الإرهاب، حيث تصل خسائر الأنظمة المستهدفة إلى مليون ضعف ما أنفقته المنظمة الإرهابية. ولا يتردد زعيم القاعدة «أسامة بن لادن» في تأكيد ذلك إذ يقول «إننا نواصل سياستنا لاستنزاف أمريكا حتى مستوى الإفلاس، وهذا يعني أن كل دولار تدفعه القاعدة يقابله بإذن الله مليون دولار تخسره أمريكا بالإضافة إلى فقدان عدد هائل من الوظائف».

بهذا أعادت القاعدة كتابة قواعد اللعبة وحددت استراتيجيتها، وحققت حتى الآن نجاحات متكررة. والهدف الثاني هو زعزعة الثقة بين المواطنين والدولة[٢٨]. وبهذا دخلت

في حرب من طراز جديد، وهو الحرب من أجل فكر، وليس لاحتلال أراضٍ أو تكوين حكومات، ليس الآن على أي حال، وهذا حقق للقاعدة مكسبين مهمين، أو لها: أن القاعدة تحارب في الظلام متخفية بين المجتمعات المدنية، مما يجعل القضاء عليها في غاية الصعوبة. المكسب الثاني والأهم: أن عناصرها، وهم الذين يؤمنون بفكرها، منتشرون في كامل الكرة الأرضية وبمستويات علمية وثقافية متنوعة، وتغطي إلى حد كبير جميع التخصصات التي يحتاجها أي تنظيم. والثالث: الممارسات غير الأخلاقية، التي تمارسها الدول الغربية ضد العالم الثالث، والتي لا يمكن تجاهلها أو إنكارها. وهذا حقق للقاعدة ميزات عدة، أهمها: خلق هيكل تنظيمي دقيق في الظل، يضاهي تنظيمات الدول ويشمل هيكلها التنظيمي ما يوازي وزارة المال والاقتصاد والتجارة والمخابرات والإعلام وغير ذلك. وعمدت المنظمات الإرهابية إلى نشر عناصر ومكونات كل فئة من هذه الفئات في جميع أنحاء العالم، دون أن يكون هناك أي اتصال مباشر بين خلاياها، كما حددت أساليب وطرق الاتصال بالقيادة العليا. لقد أتقنت القاعدة قواعد اللعبة الجديدة وعرفت نقاط الضعف في المجتمع الدولي، وركزت على تحقيق أكبر ضرر في الاقتصاد، وعلمت علم اليقين أن الاقتصاد مبني على البنية التحتية في أي دولة. كما علمت ـ أيضاً ـ أن شبكات الاتصال والحواسيب، التي تتحكم في تشغيل وصيانة شبكات البنية التحتية، هي العصب المهم في منظومة البنية التحتية، فسعت إلى جمع المعلومات التقنية الدقيقة عن شبكات البنية التحتية في جميع قطاعاتها وفي جميع الدول، وجندت المتخصصين لدراسة ثغراتها الأمنية، وتسعى باستمرار إلى تحديد النقاط القاتلة، وهي كما شرحت سابقاً، عبارة عن النهايات الطرفية أو مفاصل الشبكة، التي تتحكم فيها وتكون مسؤولة عن توزيع الأحمال وتشغيل أنظمة الحواسيب في الشبكة، والتي تعد «الموقع القاتل للشبكة» واعتبرتها القاعدة من أهم القضايا التي يبحثون عنها، سواء كانت في أنظمة البنية التحتية، أو أنها في الأسواق الاقتصادية، ويتم تحديدها في العادة من قبل مجاميع سرية ومتخصصون يعملون في المنطقة المستهدفة. ويتركز البحث في تحديد موقع في النظام ينتج عن تخريبه تعطيل شامل في النظام المستهدف، يؤدي إلى خسائر اقتصادية كبيرة بهدف زعزعة الثقة لتحقيق انخفاض في قدرات السوق وحصول فوضى سوقية مؤثرة.

والمزعج في هذا الإطار، أن قادة الإرهاب الدولي يتعلمون بسرعة ملحوظة كيفية اكتشاف «الموقع القاتل للشبكة»، ويخططون لمهاجمتها. ويبدأ التخطيط بالتعرف على الطرفية

ذات الأحمال العالية، حيث يوجد مستوى عالٍ من الارتباط بين عدد الوصلات في أي نهاية طرفية والأحمال التي يحتويها، بالإضافة إلى أن كثيراً من شبكات البنية التحتية (مثل شبكات البترول والغاز والكهرباء) يتركز إنتاجها على حجم التدفق في الشبكة، بحيث يمكن معرفة المحطة ذات الأحمال العالية من قرب ارتباطها بنقطة التغذية الرئيسة. وفي شبكات أخرى، مثل شبكات الاتصالات، يكون أكثر النهايات حملاً في مركز الشبكة. وهناك طريقة معروفة لتعطيل النهاية الطرفية، وهي مهاجمة نقاط التوصيل التي تنبثق من النهايات ذات التحميل العالي، حيث تكون النتيجة توزيعاً للأحمال التي يحتويها الرابط إلى نهايات أخرى، مما يؤدي إلى أعطال تسلسلية. وبعض الشبكات تكون عرضة للأعطال نتيجة لنقص المخزون، كما هو الحال في مصالح الكهرباء والغاز والماء، إذ إن الهجوم على محطات التوليد أو محطات الغاز الرئيسة أو خزانات المياه أو خطوط التغذية من هذه المحطات سيؤدي إلى فشل تام نتيجة لسحب موارد من محطات أخرى لتعويض المحطة المتعطلة.

النمو المطرد في تقنية المعلومات يزيد من الاهتمام بتخريب البنية التحتية:

تنمو أسواق المنطقة العربية بوتيرة متسارعة معتمدةً على التطور التقني، في محاولة جادة لأخذ موقع متميز في الأسواق العالمية، رغم أنها لا تزال في مرحلة بناء البنية الأساسية، وكلما تزايد الاعتماد على التقنية في جميع مضارب الحياة في المجتمع، زاد اهتمام المنظمات الإرهابية باستخدامها لتحقيق مآربها. وبالتوازي فإن المجتمعات أصبحت أكثر تمسكاً بنمو وتطوير البنية التحتية والعمل على تطوير التقدم التقني واستخدامه لإنجازاته التقنية مهما واجه ذلك من تحديات أمنية. وفي هذا الإطار وعلى سبيل المثال، نجد أن قطاع النفط بمنطقة الخليج، يضخ استثمارات كبيرة ومهمة لتطوير بنيته الأساسية في عدة اتجاهات أهمها مجالات تقنية المعلومات، وبذل جهود حثيثة للتماشي مع تطور التقنية، رغم احتياجه لكم هائل من الاستثمارات المالية، مما يجعل الإنفاق في صناعاته عالية خاصةً في المجمعات النفطية، التي تتطلب وفرة الكهرباء والماء والغاز وخلافه. ويتضح اهتمام الإرهاب بقطاع النفط من حقيقة الدور الذي يقوم به هذا القطاع في دعم الاقتصاد العالمي، فعلى سبيل المثال كتبت (باميلا آن سميث، Smith Pamela Ann) في مجلة «الميدل ايست The Middle East» تحت عنوان «البنوك والأسواق في دول مجلس التعاون الخليجي، تبدو أفضل في ٢٠١٠م»، إذ توقعت: أن يكون الأداء المالي

قد تحسن بشكل طفيف في دول مجلس التعاون الخليجي في ٢٠١٠م، وفقاً لما ذكره رجال المصارف والمحللون في المنطقة، بعد عام صعب في ٢٠٠٩م، وتوقعت أن يزيد الائتمان للقطاع الخاص، رغم أن البنوك ستبقى حذرة وستبحث عن مقترضين من النوعية العالية[٣٥]. وجاء في دراسة شاملة أصدرها المصرف الوطني الكويتي في يناير الماضي، أن البنوك الخليجية تستعد للاستفادة من بيئة العمل والبيئة الاقتصادية المتحسنة، إضافة إلى الدعم الحكومي المستمر. وأكدت الدراسة أنه من خلال الموازنات الخالية من العجوزات والمخصصات التي استقرت أصلاً؛ فإن الأداء المتوقع ومؤشرات البنوك الخليجية في ٢٠١٠م يتوقع أن تتحسن مقارنة مع ٢٠٠٩م، ومع احتمال بقاء أسعار النفط قوية، فمن المتوقع أن تصل نسبة النمو في المملكة إلى ٤٪ في عام ٢٠١٠م، بينما يتوقع أن يبقي التضخم تحت السيطرة؛ ولكن هناك بعض المخاوف حول السيولة، كما في كل دول مجلس التعاون الخليجي كما يذكر التقرير. ونتيجة لارتفاع أسعار النفط في السنين القليلة الماضية، استمر النفط في دعم الناتج المحلي الإجمالي وتقوية الاقتصاد في منطقة الخليج. ولتقدم العلوم والتقنية أثر ملموس في رفع مستوى الإنتاجية وتنوعها على الصناعات النفطية ومشتقاتها، الأمر الذي يحتم مجاراة التقنية والاستفادة من مخرجاتها بصرف النظر عن أي مخاطر يمكن أن تنتج جراء ذلك.

وفي الواقع؛ فإن الاعتماد على التطور التقني يزداد يوماً بعد يوم، الأمر الذي تترتب عليه عمليات تقنية معقدة تتطلب مهارات تقنية عالية لسد ما قد ينتج من ثغرات أمنية يمكن أن يستغلها المخربون، كما أنها تتطلب استثمارات هائلة في مجال البحوث العلمية والعملية لتطوير وتجديد عملياتها، إضافة إلى ارتفاع درجة المهارات الإدارية والعمّالية المطلوبة لتشغيل هذه الصناعة. وعلى غرار قطاع النفط، شهد القطاع المصرفي خلال السنوات الأخيرة في دول الخليج نقلة نوعية في حقل التقنية المصرفية واعتماداً كبيراً على تطور تقنية المعلومات والاتصالات، التي هيأته لتدشين بنية تقنية متقدمة، مكّنته من مواجهة التحديات الاقتصادية، التي واجهتها أجزاء متفرقة من العالم.

وإذا ما تغاضينا عن المخاطر الأمنية التي تلازم الشفافية والانفتاح العالمي، يتضح أن مخاطر البنوك عامة تتمثل في مخاطر مالية ومخاطر تشغيلية. وتشكل المخاطر التشغيلية نسبة ٣٠٪ من إجمالي المخاطر، بينما تمثل المخاطر المالية النسبة المتبقية ٧٠٪، وهي تتوزع على مخاطر الائتمان والمخاطر السوقية ومخاطر تغير أسعار الفائدة. وتواجه البنوك الخليجية ـ وفقاً لكثير

من المحللين ـ العديد من المخاطر المالية لاسيما الأخطار الائتمانية والأخطار النظامية الناجمة عن التغييرات والتبادلات السوقية العالمية، وذلك كله ناجم عن تطور المعايير المحاسبية الجديدة، التي تسعى للمزيد من الشفافية. وتوجه السلطات الإشرافية للتقيّد شبه التام بالمعايير والتشريعات المصرفية العالمية الحديثة، وفي الوقت نفسه، فإنها تمارس أنشطتها التمويلية والاستثمارية في بيئة أقل تقيداً بمعايير الحوكمة السليمة؛ وخاصة جملة الإصلاحات الاقتصادية، التي هي الأخرى تعرِّضْ أنشطة البنوك للتقلب.

وتشير الإحصاءات والتقارير إلى أن معدل إنفاق البنوك السعودية على تطوير بنيتها التقنية يبلغ ٧٢٠ مليون ريال سنوياً لدعم أنظمة المكننة الأساسية، ومنتجات الدعم الفني، وخدمات الصرافة الإلكترونية، وأمن المعلومات، والشبكات الداخلية والخارجية، وأجهزة الصرف الآلي ونقاط البيع، وتطوير البنية الإلكترونية وخدمات الإنترنت والانترانت، بهدف رفع مستوى القطاع المصرفي السعودي لمضاهاة أفضل القطاعات المصرفية العالمية، وذلك بالحرص الدائم على مواكبة أحدث التطورات التقنية، لتحقيق معدلات أداء متفوقة ودائمة تؤهله لطرح العديد من البرامج الاستثمارية والمصرفية ذات العوائد المالية الجيدة، بنسب مخاطر متدنية، وذلك بهدف تعزيز ثقة العملاء في قدرة البنوك المحلية على الاستجابة لاحتياجاتهم المصرفية والاستثمارية، وتوفير الحلول المبتكرة لمتطلباتهم. وتعد خدمات الإنترنت الأبرز على صعيد إنجازات القطاع المالي، حيث استطاع قطاع المال تسخير الإنترنت لخدمة عملائه عن طريق توفير حزمة واسعة من الخدمات المصرفية والاستثمارية عبر الشبكة العنكبوتية، فتمكنت البنوك عبر مواقعها الإلكترونية، من توفير معلومات شاملة لعملائها عن البنك وعن الخدمات والمنتجات المصرفية التي يوفرها، إلى جانب ما أتاحته تلك المواقع لعملاء البنوك من إمكانية التعامل الفوري مع حساباتهم، وتنفيذ العمليات المصرفية بصورة فورية وآمنة، كتنفيذ الحوالات المالية عبر نظام «سريع»، وحوالات نظام «سويفت» بالعملات الأجنبية، والتحويل بين الحسابات داخل البنك أو إلى أي حساب معروف لدى البنوك المحلية والعالمية، فضلاً عن إمكانية تسديد فواتير الخدمات العامة، وتسديد أقساط البطاقات الائتمانية، والتعامل مع الودائع وصناديق الاستثمار، وخدمات التخطيط المالي من أي بقعة جغرافية في العالم. بالإضافة إلى ما سبق؛ فإنه يلحظ توجه الكثير من الشركات المتوسطة والصغيرة لمكننة وأتمتة أعمالها، وتمثل الشركات المتوسطة والصغيرة نحو ٦٠ ٪ من حجم السوق.

ومع ما سبق إيضاحه من فوائد؛ إلا أن هذا التطور الهائل، الذي يصب في تسهيل التعاملات البنكية الإلكترونية من أي مكان في العالم تصله خدمات الإنترنت، فهو في الوقت نفسه يصعِّب متابعة كل ما يتعلق بمكافحة غسل الأموال وتمويل الإرهاب من قبل المؤسسات المالية المسؤولة عن مراقبة التجاوزات والمخالفات المالية في العالم، وتنفيذ التعليمات والتوجيهات الصادرة من الدوائر والجهات ذات الصلة، فيما يتعلق بمكافحة غسل الأموال وتمويل الإرهاب، ويمكِّن الإرهابيين من إدارة أموالهم ونقلها من حساب إلى آخر وتصعيب متابعة ذلك.

أما في مجال تطوير قطاع التقنية في منطقة الشرق الأوسط؛ فإن إجمالي الإنفاق يقدر بما يقارب ٢٦,٦ مليار دولار، منها نحو٧٩٪ في دول مجلس التعاون الخليجي. وتحظى المملكة العربية السعودية بحصة مقدراها ٧٠ ٪ من السوق الخليجي، فيما تأتي الإمارات في المرتبة الثانية. ومع التزايد المطرد في حجم سوق التعليم الإلكتروني في السعودية، الذي وصل إلى ما يزيد عن ١٢٥ مليون دولار في بداية العام ٢٠٠٨م؛ فإن العديد من الجهات في المملكة تسعى للاستفادة من هذه التقنية. وفي مجال التعليم، فإن المملكة تخصص جانباً كبيراً من ميزانيتها لهذا القطاع، إذ تعد المدارس والجامعات نقطة انطلاق مثالية نحو إعداد الأجيال الشابة لمواجهة تحديات المستقبل. وقد بدأت وزارة التعليم السعودية مؤخراً في تطبيق مناهج التعليم الإلكتروني في المدارس من خلال تنفيذ المشروع التجريبي (الفصل الإلكتروني) (eclassroom) في خمس مدارس ثانوية في الرياض، ودُشِّن في عام ٢٠٠٨م. ومن الملاحظ أن عدداً من المدارس الحكومية والخاصة قد قامت بتبني برامج للتعليم الإلكتروني، باستخدام أحدث الأدوات والتقنيات العالمية، التي تشمل البنى التحتية التكنولوجية اللاسلكية. وتمكنت الجامعات والكليات السعودية أيضاً من تحقيق خطوات واسعة في مجال استخدام حلول التعليم الإلكتروني. ونظراً للانفتاح والشفافية العالية التي تميز الإنترنت؛ فإن أي شخص يستطيع أن يصل إلى معلومات دقيقة ودروس متخصصة للتعامل مع التقنية بصورة عامة وتقنية المعلومات على وجه الخصوص. وهذا ينطبق ـ أيضاً ـ على عناصر المنظمات الإرهابية التي يمكنها نسخ وتطوير البرامج والأدوات التي تسهل عملياتهم الإرهابية؛ بل بإمكانهم الحصول على شهادات عالية وفي أي مجال، بما فيها التخصصات النادرة مثل الكيمياء والفيزياء والاتصالات وغير ذلك، مما يجعلهم حاضرين في دائرة التعليم العالمية، ويمكنهم من متابعة

الأبحاث والدراسات التقنية.

أما في مجال التجارة الإلكترونية، فقد بادرت كثير من الدول إلى اتخاذ الإجراءات اللازمة لتنظيم التعامل وفق هذا النمط الجديد من أنماط التجارة، الذي يتميز بسرعة النمو والشمولية وحدة المنافسة وعدم الاعتراف بالحدود الجغرافية في التعامل التجاري، وعمدت إلى تطوير أساليب المراجعات المالية باستخدام النظم الآلية والتوسع في تطبيق رقابة الأداء، والاعتماد على تقنية المعلومات في عمليات التدقيق والتطوير. كما أن تلك الدول لا تتوانى في تطوير المعايير الرقابية والأنظمة واللوائح المالية والمحاسبية، بل أن الأمر قد وصل بالحكومات إلى تسهيل الإجراءات التنظيمية لتشمل العلاقات التي تحكم قطاعات الأعمال والمستهلكين، وأدت إلى نتائج وانعكاسات بعيدة المدى على الجوانب القانونية والتنظيمية، وحقوق الملكية الفكرية وحماية الاستثمارات، وغيرها من الجوانب التقنية والمالية ذات الصلة بالتجارة الإلكترونية، وحرصت على تشجيع المجتمع المدني للانتقال إلى التجارة الإلكترونية. ومن أبرز المؤشرات على تزايد أهمية التجارة الإلكترونية ما شهدته السنوات الماضية من زيادة مطردة في حجم التجارة الإلكترونية، فقد مكنت شبكة الإنترنت الأفراد والقطاعات التجارية الصغيرة والمتوسطة، وكذلك الكبيرة على حد سواء، من الاستفادة من تقنيات التجارة الإلكترونية وممارستها بأشكال مختلفة.

ويطلق مصطلح التجارة الإلكترونية على تنفيذ وإتمام عمليات التسويق والبيع والشراء عبر الوسائل الإلكترونية، ولتحقيق نجاح كامل في هذا المجال؛ فقد طرحت مؤسسة البريد السعودي عدداً من الحلول والتطبيقات البريدية، مثل السوق الإلكتروني emall، وهو عبارة عن ربط بين المؤسسات والشركات، التي تمارس البيع عن طريق الإنترنت وزبائنها من خلال توصيل البضائع بسرعة وكفاءة عالية. وكذلك فإن هذا البرنامج يسهم في دعم المنظمات الخيرية وهيئة السياحة ونقل المنتجات الحرفية، التي ينتجها المواطنون وذوي الاحتياجات الخاصة. كما أنه يسهل بيع وتوزيع المنتجات، لأنه يمكِّن المواطن والمقيم وكذلك رجال الأعمال من الحصول على عنوان بريدي في أمريكا وأوروبا وغيرها من الأسواق الدولية، لضمان سرعة وكفاءة نقل السلع من وإلى دول العالم. وتمشياً مع متطلبات التعاملات الحكومية في المملكة؛ فقد وقعت مؤسسة البريد السعودي اتفاقيات مع عدد من المصالح الحكومية، وعلى رأسها وزارة الداخلية، بهدف تنشيط التعاملات الحكومية. وتعد شبكة الإنترنت من أكثر الوسائل

الإلكترونية استخداماً لهذا الغرض.

وقد أصبح للتجارة الإلكترونية تأثيرات جوهرية في أسلوب إدارة الأنشطة الاقتصادية، وممارسة الأعمال التجارية وما يتصل بها من خدمات. وفي ما يتعلق بإمكانية استفادة الإرهاب من التسهيلات الملازمة لهذا النوع من التجارة فهي واضحة، إذ يمكن الحصول على بطاقات ائتمان مسبوقة الدفع عن طريق الإنترنت، كما حصل في قضية اغتيال الزعيم الفلسطيني محمود المبحوح، حيث استخدم الإرهابيون الصهاينة بطاقات صادرة من بنوك عالمية على أساس الدفع المسبق. ويمكن استخدام عناوين مؤقتة لشراء برامج وأدوات؛ بل وشراء كثير من السلع. كما أن بعض المؤسسات المتعاطفة مع الإرهاب يمكنها استخدام شبكات النقل العالمية لإيصال الطرود والبضائع الممنوعة بكل يسر. ومن الأساليب الخبيثة التي يستخدمها لصوص الإنترنت، هو ما سبقت الإشارة إليه بما يعرف بالهندسة الاجتماعية، أو الاصطياد، وذلك عندما يستجيب المواطن لطلبات مشبوهة ترسل من قبل غرباء ينتحلون صفة البنوك، فيكشف العميل لهم معلوماته الشخصية أو المصرفية، التي يتم استغلالها فيما بعد لتنفيذ عمليات احتيالية، وهي مشكلة حقيقية في العالم كله، علماً أن معظم العمليات، التي يتعرض لها عملاء البنوك سببها عوامل ترتبط بالإهمال من قبل الضحية. وبسبب تزايد الاعتماد على التقنية كالحواسيب والإنترنت والأجهزة الإلكترونية المصرفية، مثل أجهزة الصراف الآلي ونقاط البيع؛ نجد أن منافذ الخدمات الإلكترونية المصرفية تستحوذ على نصيب الأسد ضمن عمليات الاحتيال التي يتعرض لها عملاء البنوك. ولضمان نجاح أي مشروع للتجارة الإلكترونية، لابد من الأخذ بعين الاعتبار عدداً من الأسس، التي تساعد على الاستفادة القصوى من الفرص التي تتيحها تقنيات التجارة الإلكترونية، مثل تنمية القدرات المؤسسية، وتفعيل وسائل المراجعة الداخلية في الأجهزة الحكومية، وتعزيز التعاون والتواصل بين الأجهزة الحكومية والأجهزة ذات الصلة داخلياً وخارجياً، لضمان سد الثغرات التي تساعد الإرهابيين والمفسدين. ومن الضروري الحرص في أن تتوافق أهداف التجارة الإلكترونية مع التوجهات العامة للتنمية، وحماية النزاهة، ومكافحة الفساد، وتنويع النشاط الاقتصادي، وتقديم الخدمات للمواطن بيسر وسهولة، من خلال الإسهام في رفع كفاءة الأداء في الأجهزة الرقابية وتمكينها من تحقيق أهدافها لتلبية متطلبات التنمية وتحقيق الانضباط المالي والإداري. وتتمثل مهام الدولة في الرقابة المالية على جميع إيرادات الدولة ومصروفاتها، ومراقبة كافة أموال الدولة المنقولة

والثابتة والمال الخاص والعام بهدف محاصرة غسيل الأموال وضمان القضاء على أي تعاملات مشبوهة، ويتطلب ذلك إعداد تقييم موضوعي سنوي عن الإدارة المالية للدولة، ولكل جهة حكومية في القطاعين الحكومي والخاص، ومراقبة حسن استعمال الأموال واستغلالها والمحافظة عليها، ورفع تقارير مهنية وموضوعية ذات مصداقية عالية لأعلى مستويات الدولة حول أداء الأجهزة الخاضعة للرقابة.

التحكم الآلي والبنية التحتية المحلية:

تعد أنظمة التحكم الإلكتروني في حياة المجتمع بصورة عامة، وفي شبكات البنية التحتية على وجه الخصوص؛ من المكونات الضرورية التي أصبحت جزءاً من الحياة الحديثة، التي لا يمكن للمجتمع الاستغناء عنها. ومع ذلك، فإن كثيراً من الناس لا يعيرون أنظمة التحكم تلك الاهتمام اللازم، رغم أنهم يستخدمونها بانتظام، منذ أن استيقاظهم من النوم صباحاً وحتى عودتهم إليه مرة أخرى، فمن ذا الذي لم يستخدم جهاز التحكم في درجات الحرارة الموجود تقريباً في كل مبنى في المملكة لغرض تسخين الماء إلى درجة مختارة، أو التحكم في درجة حرارة الغرفة، ونظام ضبط السرعة في السيارات، ونظام التحكم في الكاميرات. كل هذه الأنظمة تنظم آلة أو جهازاً لتحقيق مهمة محددة، كأن تطفئ سخانات المياه عند ارتفاع الحرارة، أو توقف تبريد المكيف عندما تصل درجة حرارة الموقع إلى الدرجة المرغوبة. كما أن نظام ضبط السرعة في المركبات يضيف الوقود لمحرك السيارة عند انخفاض السرعة، وتصغير فتحة الكاميرا وزيادة وخفض سرعة الغالق عند ارتفاع مستوى الإضاءة إلى آخره. إن جميع أنظمة التحكم، التي تتحكم في تشغيل أي آلة أو محرك أو مصنع بأكمله تسمى نظام تحكم آلي، وتعرف بأنها «أتمتة أو مكننة»، أو التحكم الإلكتروني Cybernetics (وقد تم توضيح الفرق بين اصطلاح المكننة والأتمتة في الباب الأول)، وكلاهما يستخدم تغذية مرتدة feedback. وبعبارة أخرى؛ فإن المكننة عبارة عن استخدام قياس المخرجات الآنية للتحكم أو التأثير على المدخلات المستقبلية، وذلك لتحقيق الاقتراب من حالة مرغوبة. وتعد الإشارات الإلكترونية التي تمثل هذه القياسات ومدخلات التحكم حجر الزاوية في عالم التحكم الحاسوبي.

وبنظرة شمولية، فإن التحكم في أي عملية تشغيلية لأي آلة بواسطة إشارات إلكترونية

يمثل تطبيقاً عملياً «للمكننة والأتمتة»، وبهذا المعنى تصبح شبكات الحواسيب جوهر التحكم الآلي في أنظمة البنية التحتية الوطنية، بما فيها شبكات نقل وتوزيع الطاقة الكهربائية، وشبكات المياه، ومحطات ضخ البترول من مصادره إلى الموانئ في شرق البلاد وغربها، ومرافق جوهرية أخرى يصعب حصرها. وعندما يستهدف قراصنة الحواسيب أجزاء حرجة من شبكات البنية التحتية على المستوى الوطني، فإنهم سيتسببون حتماً في تعطيل محطات توليد الكهرباء، أو التسبب في فيضانات عند تعطيل النظام الآلي لتوزيع الماء في المدن، أو تسريبات الزيت من أنابيب النقل والتوزيع. ولا تتردد حكومات العالم بالاعتراف بأنها متخلفة عن إمكانيات القراصنة في هذا المجال؛ حيث تشير دراسة نشرتها شركة مكفي McAfee Inc في يناير عام ٢٠١٠م، بناءً على مسح شمل ٦٠٠ مدير تنفيذي ومدراء تقنيين لمشغلي مرافق البنى التحتية في ١٤ دولة، أوضحت هذه الدراسة نظرة لم تكن في حسبان الحكومات والمجتمعات المدنية وأظهرت مستوى الأضرار، التي يمكن أن يسببها القراصنة للمرافق المهمة، مثل شبكات ومحطات توليد الكهرباء، وأنظمة المياه وتصريف السيول والصرف الصحي، وأنظمة التحكم في نقل البترول والغاز عبر الأنابيب، أو مصادر تحميل بواخر نقل البترول العملاقة، حيث أفاد أكثر من نصف المشغلين لشركات الكهرباء ومرافق البنى التحتية الأخرى، الذين شاركوا في المسح بقولهم إن أنظمة حواسيبهم قد اخترقت من قبل هجوم خبيث ومتقن. ويشير التقرير إلى أن ٥٤٪ من مسؤولي البنى التحتية اعترفوا أن باستطاعة المخربين غرس برنامج خبيث لسرقة البيانات والملفات المهمة، والتجسس على المراسلات والبريد الإلكتروني، والتحكم عن بعد بالأجهزة الموجودة في المرافق المستهدفة. ومما سَهَّل مهمة المخترقين أن جميع المرافق تستخدم في الوقت الحاضر برمجيات شائعة ومعروفة، وتربط أجزاء من معدات الشبكة مع الإنترنت بهدف تمكين مهندسيها وفنييها من إجراء أعمال الصيانة عن بعد، الأمر الذي يفتح الباب أمام القراصنة للوصول إلي النظام. وبالنسبة نفسها أفاد المشاركون في المسح الإحصائي أنهم تعرضوا لمستوى عالٍ من تعطيل الخدمات، بسبب تعطيل الحواسيب التي تؤدي الخدمات عن طريق إغراقها بحمولات زائدة عن طريق الإنترنت؛ وكثيراً ما وجه مشغلو البنى التحتية اللوم لدول أجنبية لها مصالح في منع الخدمات. ومما يثير القلق والانزعاج في التقرير؛ أن شبكات الطاقة وشبكات نقل البترول والغاز تعد من أكثر الأهداف التي يهاجمها القراصنة للحصول على فدية للتوقف عن تخريبها. وكما تم شرحه في فصول سابقة؛ فإن كشف الاختراقات وتحديد القراصنة في منتهى الصعوبة، وذلك بسبب ما يقوم به القراصنة من العبث في عدد من

الحواسيب ويسلكون طرق وشبكات متعددة بهدف التمويه، إلا أنه ببحث متقن وإصرار كبير من قبل الجهات المعنية بمحاربة القرصنة، يمكن في أحيان كثيرة تحديد المهاجم والبلد الذي نشأ منه الاختراق.

إن الجزء المتعلق بالحوسبة في البنية التحتية بما في ذلك أجهزة الحواسيب والبرمجيات وروابط الاتصالات والمعلومات المعقدة المضمنة فيها، هي التي تمثل النظام العصبي للبنية التحتية التي تعتمد عليها الدول والمجتمع بأسره. وتتميز جميع قطاعات البنية التحتية وأنظمة المكننة المساندة لها بصفات تميزها، تُزيد من حجم الأضرار التي يسببها القراصنة لو تمكنوا من تعطيلها؛ فقطاع الطاقة يوفر عدداً من مكونات الحياة الحديثة التي أصبحت جزءاً من الضروريات، التي لا غنى للمجتمع عنها، فهي تنقل الطاقة على هيئة كهرباء ووقود وغاز طبيعي، ولها محطات وإنشاءات تشمل محطات إنتاج وشبكات توزيع ومحطات فرعية وتعطيل هذا القطاع الحيوي سيعيد أي مجتمع لعصر ما قبل الثورة الصناعية. وفي قطاع الطاقة تتكون شبكة المكننة من «تحكم رقابي ومعدات استحصال البيانات وروابط الاتصالات»، وجميع هذه العناصر تتحكم في المفاتيح والصمامات والمضخات في كامل نظام التوزيع. وكثيراً ما تستخدم روابط الاتصالات نفس خطوط التوزيع وصلاحيات الوصول التي تستخدمها البنية التحتية الشاملة.

أما في قطاع الاقتصاد والمال؛ فإن التعاملات الإلكترونية في البنية التحتية للخدمات المالية تمثل أساس الدعم للاقتصاد الوطني، كما هو الحال في عمليات القطاعات الأخرى، لأن هذا القطاع يعتمد بشدة على روابط الاتصالات وقواعد معلومات حاسوبية منتشرة في جميع أنحاء العالم. وتستخدم الشبكات الإلكترونية بثقل كبير لتحويل الموارد المالية بين المستهلكين والمؤسسات التجارية وبين الشركات فيما بينها والتعاملات البنكية والتحويلات الحكومية، بما فيها رواتب الموظفين في الحكومة أو في القطاع الخاص. أما فيما يتعلق بالبنية التحتية لقطاع النقل، فبالإضافة إلى توفير تنقلات وسفر المجتمع؛ فإنها تنقل البضائع والمنتجات الزراعية والبريد والطرود البريدية، التي تعد شرايين الحياة للتجارة. ويستخدم هذا القطاع شبكات المعلومات في المراقبة الجوية وتوجيه الطائرات، ومتابعة تحرك سيارات النقل في شركات النقل الكبيرة، مثل شركة «ناقل» التي تجوب أنحاء المملكة لنقل البريد والبضائع، وغير ذلك من السلع مستخدمة أنظمة تحديد المواقع، والمتابعة الإلكترونية.

أما البنية التحتية للاتصالات، فتعد فريدة مقارنة ببقية القطاعات، إذ إنها لم تصمم فقط لنقل الخدمات وتوفير الاتصال بين الناس، ولكنها تتضمّن قنوات الإشارات، التي تعتمد عليها القطاعات الأخرى لنقل معلومات التحكم الآلي الخاصة بها. والشيء نفسه بالنسبة لنظام الهاتف، إذ إن البنية التحتية للاتصالات وشبكة نظام التحكم الآلي هي المسؤولة عن التحكم في توجيه وتوزيع المكالمات والرسائل ونقلها إلى الوجهة الصحيحة، وكذلك المقاسم والإشارات التي تتحكم في الوصلات والروابط الأخرى. وبشمولية أوسع؛ فإنه يمكن القول أنها تشتمل على شبكات معلومات الشركة الداخلية وقواعد المعلومات، التي تستخدمها شركات الاتصالات لدعم عملياتها وأعمال الصيانة والتشغيل والإدارة، وكذلك توفير الخدمات الكثيرة الأخرى، التي تميز شركات الاتصالات اليوم، والتي أصبحت رقمية ولاسلكية ومزوِّدة للنطاق العريض عن كونها مجرد شركات لتوفير الهواتف فقط.

وإلى جانب هذه الصفات والمميزات التي يتميز بها كل قطاع من قطاعات البنية التحتية؛ فإن هناك ميزات مشتركة بينها، إذ إن جميع هذه القطاعات تخدم نطاقاً واسعاً من المشتركين، وحصول عطل شامل في أي منها قد يؤدي إلى عواقب وخيمة على مستوى واسع يطول الصحة العامة والأمن الوطني وقطاع الطاقة والاقتصاد. فالترابط المشترك بين قطاعات البنية التحتية كبير جداً وتبادلي بين جميع قطاعات البنية التحتية والتنموية وشبكات الاتصالات التي تساندها، حيث إنّ شبكة الهاتف تعتمد على شبكات الطاقة الكهربائية في معظم أجزائها، وتعتمد شبكات الطاقة الكهربائية على قطاع النقل لتوصيل الوقود، في حين أن جميع القطاعات تعتمد على قطاع الاتصالات وعلى البنية التحتية للتعاملات الاقتصادية. وبهذا فإن معظم القطاعات تستفيد من شبكة الهاتف العامة لنقل بعض أو جميع قنوات التحكم الآلي الخاصة بها، كما أن معظم شبكات التحكم لها بعض الارتباط مع الشبكات العامة بصورة عامة، وأكثرها من خلال شبكات الإنترنت. إضافة إلى ذلك فإن هناك اتفاقيات السماح بالوصول أو المرور بين القطاعات والمؤسسات في كثير من المواقع المنتشرة في أرجاء العالم. والبنية التحتية بطبيعتها محلية وإقليمية وعالمية في نطاق نشاطها، لذلك نجد أن كل قطاع له أجزاء وعناصر منتشرة في أنحاء البلاد، وربما تمتد إلى الدول الإقليمية والعالم.

والواقع أن معظم قطاعات البنية التحتية مملوكة للقطاع الخاص بصورة منفردة أو بالمشاركة مع الدولة، وخاصة بعد أن اتجهت كثير من الدول للخصخصة. ويوجد تنسيق

بدرجات متباينة بين مقدمي الخدمات في القطاعات المختلفة، ولكن ليس هناك سلطة مركزية تربط جميع هذه القطاعات، والمتوافر هو هيئات تعتني بقطاع محدد. ولو أخذنا المملكة العربية السعودية على سبيل المثال، نجد أن هيئة الاتصالات وتقنية المعلومات تنظم قطاع الاتصالات، وهيئة سوق المال تنظم قطاع المال والاقتصاد، وهكذا. ولذلك فإن أساليب تحقيق الاعتمادية في كل قطاع منفصلة تماماً وتختلف من قطاع إلى آخر، من كونها تطوعية في بعض القطاعات إلى نماذج مختلفة من الشراكة بين القطاع الخاص والحكومة، وبعض التنظيمات والتشريعات الحكومية هي المألوف في جميع القطاعات، رغم التوجه العام الذي يتزايد هذه الأيام نحو تقليص تدخل الدولة.

ولم ينته الأمر عند البنية التحتية؛ بل تعداه ليشمل التعاملات الإلكترونية الحكومية، إذ إن الحكومات تسعى بخطى حثيثة، من منطلق مواكبة التطور التقني، وفي إطار التحديث والتنظيم، لتطبيق الحكومة الإلكترونية، بهدف تسهيل التعامل بين الحكومة والمواطنين، وكذلك السعي إلى رفع مستوى خدمات البنية التحتية في المكننة والتمهيد للحكومة الإلكترونية والتجارة الإلكترونية، فأطلقت كثير من الدول برامج التعاملات الإلكترونية والمكننة بهدف زيادة الفعالية والإنتاجية والشفافية في العمل الإداري ومواكبة التطورات في هذا المجال وتقديم الخدمة، سواء للمواطنين أو ضمن إطار العمل الإداري بأقصر وقت وبأكبر إنتاجية ممكنة. وقامت جميع الهيئات والوزارات المعنية بالتقنية في كثير من دول العالم بتشجيع ومتابعة مكننة كافة المعاملات الإدارية في دوائر ومصالح الدولة؛ مما أضاف بعداً جديداً يستلزم توقي الاختراقات، والأخذ بأسباب حماية بيانات ومعلومات الحكومة الحساسة باستخدام آخر ما توصلت إلية التقنية الحديثة، وكذلك سن التشريعات والقوانين المتعلقة بجرائم القرصنة الإلكترونية.

الفصل الثاني

اعتمادية الشبكة والسياسات العامة

الفصل الثاني

اعتمادية الشبكة والسياسات العامة

رغم خضوع معظم البنية التحتية اليوم لسيطرة القطاع الخاص؛ إلا أنه من المهم جداً أن تستمر الدول في مسؤوليتها لتحقيق رفاهية وازدهار المجتمع، لضمان تقديم واستمرارية الخدمات، التي تحقق الصالح العام في جميع أنحاء البلاد. ومنذ عقود، تسعى الدول للتعاون مع القطاع الخاص، لتوفير المستوى المطلوب من الخدمات العامة بأسعار معقولة وإمكانية وصول متساوية بين أفراد المجتمع. ومع إدراك وجود الثغرات، التي تكمن في أنظمة وشبكات التحكم الآلي، فإنه لابد أن يأخذ موضوع الاعتمادية مكانه المناسب، كهدف مهم في السياسات العامة للمحافظة على استدامة عمل شبكات البنية التحتية والتنمية الوطنية. ومن الضروري - أيضاً - تحديد أهداف الاعتمادية بوضوح لتوفير بنية يمكن الاعتماد عليها لمقاومة التحديات المتوقعة دون إخفاق ودون توقف وبتكاليف معقولة. ولا شك أن مثل هذا الهدف قد يكون من الأهداف طويلة الأمد في السياسات العامة للدول.

والواقع التاريخي يشير إلى أن القطاع الخاص كثيراً ما يأخذ زمام المبادرة لتحديد وتلبية متطلبات أهداف الاعتمادية في معظم قطاعات التنمية والبنية التحتية.

ولا شك أن مثل هذه الاتجاهات تحقق أعلى النجاحات؛ لأن أي قصور في الاعتمادية يؤثر

بصورة مباشرة على الشركات إما بتعطيل بعض الخدمات، التي تجلب العوائد المالية للشركة، أو بإنقاص ثقة العملاء وولائهم، لهذا؛ فإنه من المتوقع والضروري أن تستمر الشركات في التعامل مع تهديدات الاعتمادية المؤكدة، مع أن جميع القطاعات والصناعات تخضع في الوقت الحاضر لتغيرات سريعة للغاية. فالشركات هذه الأيام تعيد هندسة وتقليص الدخول لمقدمي الخدمات الجدد، بسبب رفع المراقبة الحكومية أو خفضها، كما أن تطبيقات تقنيةْ شبكات الحواسيب غير المقيدة تقريباً، تفرض ضغوطاً جديدة على ما كان يعد خدمات عامة ثابتة. والمهم هذه الأيام هو إدراك ما إذا كانت الأسواق ستلاحظ وتحد ـ بما فيه الكفاية ـ من قصور الاعتمادية في بيئة متغيرة للغاية؟ أو أن البلاد ستتعرض في يوم ما إلى إخفاق شامل في خدماتها الأساسية لتتحرك، وتحشد جميع الإمكانات لحل الكارثة كما هي العادة؟.

إن أدوات السياسات التقليدية المتوفرة للحكومة للعمل مع الأسواق التجارية، بهدف إدراك الأهداف الوطنية، مثل التشريعات واللوائح التنظيمية والتراخيص وجميع المحفزات الأخرى، جميعها يوفر بدائل مهمة في ساحة الاعتمادية. ومع ذلك فإنه لا يمكن أن يكون أي منها مؤثراً، إلا إذا وجد إجماع على تحديد ما يجب أن يكون عليه «مستوى الاعتمادية»؟ وتعريف ما هي «التهديدات»؟ وما هي «المخاطر المقبولة»؟ وما هي «الإجراءات الوقائية» الواجب اتباعها؟ وكيف يمكن اعتماد «التكاليف» وكيفية توفيرها؟. والملاحظ حالياً أن البت في هذه التساؤلات بعيد جداً، وحتى مرحلة إدراك بوادر حدوث نقص الاعتمادية في القطاعات المختلفة لازال غير معروف، أو لم يحدد بوضوح، ولذا؛ فإن الاهتمام بوضع سياسات إضافية قد يساعد في الإجابة عن هذه الأسئلة الصعبة، ولكن الإجماع العام لإدراك المشكلة، هو الإجراء الفعال في نهاية المطاف. والجزء المهم من مسؤوليات الدول هو تنشيط الحوار الوطني في مجال الاعتمادية، وتوفير وسائل لتحقيق إنجاز مثمر في السياسات العامة.

ولهذا فإنه من مسؤوليات الدول إقامة الندوات وورش العمل وتكوين هيئات متخصصة تعمل حصراً لدراسة الاعتمادية والإجابة عن جميع التساؤلات المتعلقة بها وتحديد دقيق للتهديدات والمخاطر. ويجب جمع كل مقدمي الخدمات العامة وموردي ومصنعي الأجهزة وخبراء التقنية وواضعي المعايير والمواصفات والوزارات والهيئات المعنية بالتقنية والتنمية والبنية التحتية في ندوات عامة لتطوير الاقتراحات والسياسات لدعم اعتمادية الأنظمة والشبكات. ومن واجبات الدول ـ أيضاً ـ أن توجد أجواء تشجع على رفع مستوى

الاعتمادية في البنية التحتية من خلال مبادرات القطاع الخاص، ويمكن أن تقوم بدور حيوي بتبني الإبداعات والتخصيص والعمل مع الصناعات لتطوير معايير فنية، وتشجيع تطوير أساليب القياس والتوثيق والتصديق على مستويات الاعتمادية (كأن تصادق على أن شركة ما حققت مستوى ٩٥٪ من الاعتماد على شبكاتها)، وتسهل على الصناعة ومقدمي الخدمات عمل تطوير وتحديث للاعتمادية. وبإمكان الحكومة أن تسهم بكل إمكاناتها الأمنية والصحية وإدارات الأمن والسلامة في تحديد الثغرات، وتصنيف تحديات الاعتمادية، التي تسببها الكوارث الطبيعية والتقلبات الجوية، وتحديد الأنشطة في جميع هذه النطاقات وممارستها سيؤدي حتماً لرفع مستوى الإدراك واليقظة المستمرة للسياسات العامة.

إن التحرك السريع والجاد بين جميع المعنيين بأمن وسلامة شبكات البنية التحتية بكافة أنواعها في القطاعين الحكومي والخاص، أمر مهم وأساسي لوضع مسألة الاعتمادية في إطارها الصحيح. ولإجابة السؤال المتعلق بالاتفاق على أقل مستوى للاعتمادية يمكن قبوله، ولضمان استمرارية اهتمام مناسب للمجتمع في هذا الموضوع؛ فإنه يلزم على الجهات الحكومية المعنية بشبكات البنية التحتية أن تساعد في توفير إرشادات ملزمة لجميع صناع التقنية ومقدمي الخدمات لتنسيق الجهود لرفع مستوى الوعي والاعتمادية في جميع الشبكات، وعلى وجه الخصوص تلك التي تحمل إشارات التحكم الآلي. وكذلك تمتد السياسات العامة لاستثمارات الدول في البحوث والتطوير، ومن الضروري أن تتبنى الجامعات بصورة عامة، وجامعة الملك عبدالله في المملكة العربية السعودية بصورة خاصة، إجراء البحوث التي تسهم في رفع الاعتمادية في جميع الشبكات الحيوية والإلكترونية.

ويمكن تعزيز الاعتمادية بفرض تشريعات ترسم الخطوط العريضة، وتحدد الأنشطة والتصرفات المسموح بها عند استخدام الشبكات الإلكترونية التي تخدم المكننة. وقد يكون، وقد لا يكون من السهل تطبيق مثل هذه الإجراءات نظراً للامتداد العالمي، الذي تفرضه طبيعة شبكات المعلومات وتقنية الإنترنت؛ فالمسافات لا تعيق المتجاوزين والخارجين عن القانون أو الإرهابيين من الوصول ومحاولة التخريب، إلا أن سن القوانين والتعاون الدولي للحد من عبث قراصنة الحواسيب أمر في غاية الأهمية.

وأخيراً؛ فإنه ومن مصلحة الحكومات العمل الجاد والتعاون لتطبيق قوانين محاربة

القرصنة الإلكترونية، وتطبيق تعليمات رفع الاعتمادية في الشبكات العالمية. وبالمثل فإن التهديدات، التي تتعرض لها شبكات المعلومات والتحكم الآلي تمثل تحديات تتقاطع مع مهام إدارات ووزارات متعددة، مثل وزارة الدفاع والداخلية (بجميع إداراتها المختلفة) والاستخبارات العامة والوزارات المعنية بالتنظيمات التقنية، مثل وزارة الاتصالات وتقنية المعلومات، وهيئة الاتصالات وتقنية المعلومات، ومدينة الملك عبد العزيز للعلوم والتقنية، مما يؤكد ضرورة التنسيق الدائم وعقد المؤتمرات وورش العمل لدعم وتنسيق الجهود التي ترفع من مستوى الاعتمادية وتحقق المصلحة العامة.

طبيعة البنية التحتية والتحديات التقنية نتيجة نمو التطور التقني

إن شبكات المعلومات المساندة للبنية التحتية معقدة للغاية، كما أنها مستمرة في النمو والتطور بتسارع ملموس، وهي ليست نتاج تصميم واحد متكامل، ولكنها تطورت تدريجياً مع الزمن، ولا زالت تواصل النمو والتوسع والتعقيد بإضافة تقنيات وخدمات جديدة. وفي هذا الفصل سيتم التعرف على بعض التحديات التقنية الموجودة في شبكات البنية التحتية بجميع أنواعها، واستعراض مفاهيم توضح بعض الاحتمالات المتوقعة للأعطال الشاملة. ولأن معظم شبكات المكننة الآلية العاملة اليوم عبارة عن مجموعة من الشبكات المترابطة والمستقلة عن بعضها بعضاً؛ فإن التراسل فيما بينها في غاية الأهمية لرفع فعالية الشبكة؛ بل إنه جوهر أدائها. وعندما يتعامل النظام مع بيئة مادية حقيقية؛ فإنه يصعب التنبؤ بالتعاملات التي تتم فيما بين الأنظمة الفرعية، لكونها غير منتظمة وليست تسلسلية، كما هو الحال في خطوط الإنتاج، ولكنه يمكن أن يكون عشوائياً وغير متزامن وغير متوقع، لأن كثير من التعاملات تولد تلقائياً بواسطة الحواسيب، التي تنفذ برامج تعتمد على الاستدلال المنطقي. وكثيراً ما يستخدم اصطلاح «الذكاء الصناعي» لوصف مثل هذه الإجراءات، ويمكن أن يكون هذا الاصطلاح صفة مناسبة تنطبق على الطبيعة الذاتية لأنظمة التحكم الآلي.

وفي الغالب، فإن أنظمة التحكم الحاسوبي الفرعية تقاوم أي تغيير في تسلسل الأوامر والمحتويات والتزامن، وينطبق هذا بصورة خاصة، عندما تكون التغييرات متعلقة بأنظمة أخرى من الشبكة. فنشوء هامش صغير في الباب الخلفي في أي نظام من النظم المترابطة، قد يتسبب في ثغرة خطيرة تؤدي إلى تفاعلات وردود أفعال تسلسلية. وتسمى الأنظمة الفرعية،

التي تعمل بهامش صغير بأنها أنظمة مقترنة أو متوائمة بإحكام «Tightly Coupled»، وهو أمر طبيعي في شبكات الحواسيب المعقدة. وتعمل أنظمة التحكم الحاسوبي في البنية التحتية بطبيعتها بانتظام ودون توقف، لتتحكم في عناصر وأنظمة مادية آنياً، ولتخدم في نهاية المطاف الأفراد والهيئات. ومن الضروري التعامل مع مدخلات عشوائية متزامنة من مصادر كثيرة وتتعامل مع عدد هائل من المكالمات الهاتفية والتعاملات الاقتصادية وخطط الطيران لآلاف الرحلات الجوية، بالإضافة إلى مدخلات المدراء في جميع الشبكات. كما أن أنظمة التحكم المهيأة لاستخدامات معينة، لابد لها من التعامل مع مدخلات غير معتادة؛ بل غير متوقعة.

ومما ينبغي ملاحظته أن الضغط على شبكات الهاتف في الأعياد والمناسبات الوطنية والدينية يتسبب في خروج النظام من الخدمة، وعجز النظام عن التعامل مع الكم الهائل من الرسائل والمكالمات. وعلى الدوام يعد العنصر البشري عنصراً أساسياً في أنظمة التحكم الحاسوبي؛ فمن المستحيل الاستغناء عن القرارات البشرية، ولا يوجد أي نظام آلي مصمم ليعمل تماماً بمفرده ودون تدخل البشر. لهذا؛ فإن احتمال وقوع الأخطاء البشرية أثناء تشغيل النظام المعقد أمر لا يمكن تلافيه. ومن الواضح أن تعقيدات وسرعة التعاملات بين عناصر الشبكات يمكن أن تتجاوز بسهولة قدرة المشغلين على تقدير المشاكل والاستجابة لها؛ فالمجسات وأجهزة الاستشعار والمؤشرات الإلكترونية وشاشات العرض المتوافرة، بالإضافة إلى إمكانية إدخال الأوامر والوقت المسموح به، هو الذي يشكل التدخل البشري. وكثيراً ما يربط المستخدمون نظامين مستقلين عن بعضهما متسببين في إنتاج تغذية ارتدادية Feedback مفاجئة، ومكونين احتمالات جديدة لتعاملات أنظمة فرعية غير متوقعة. إن إيجاد توازن صحيح بين التحكم البشري والآلي يعد مشكلة فنية تؤثر في صلب تحديات اعتمادية الشبكات، مع أن سلامة عناصر الأجهزة وروابط الاتصالات وصحتها متطلبات أساسية في اعتمادية أي شبكة. كما أن تعريض العناصر الإلكترونية للعوامل الجوية والواجبات اليومية والتقادم في عمر الأجهزة يفرض إجهاداً لا يمكن تلافيه على معدات البنية التحتية. وأخيراً؛ فإنه لابد لنظام التحكم الحاسوبي من أن يرتبط بمعدات كهربائية متحركة Electromechanical مثل السويتشات والبدالات والصمامات والمحركات Motors، التي تجعل البنية التحتية فاعلة، ومن متطلبات هذه المعدات أن تكون متينة لتقوم بوظائف متنوعة وتستمر في العمل لأطول فترة ممكنة رغم تآكلها.

إن أحد الدوافع المهمة لاستخدام شبكات المعلومات للتحكم في أنظمة البنية التحتية هو تسهيل الوصول إليها وجعلها أكثر قبولاً للمدخلات الإدارية، إلا أن تسهيل إمكانية الوصول يصعب تقييدها فور تطبيقها؛ فعلى سبيل المثال يلحظ أن كثيراً من الشبكات تحولت لتقنيات عامة، مثل تقنية الإنترنت على وجه الخصوص، مع أنها لم تصمم لتحظى بدرجة عالية من الأمن، لأسباب تتعلق بالتكلفة، ولأنها كانت تعمل في بيئة عمل مغلقة. وكلما أصبحت تقنية الشبكة عامة أكثر، كانت معروفة أكثر ومستغلة أكثر، وهنا مكامن ضعفها. إضافة إلى ذلك؛ فإن التوجه نحو تهيئة قياسية للنظام، تؤدي إلى تسهيل مهمة المهاجمين. وقد أصبح الربط بين الأنظمة العامة وأنظمة الشركات والمؤسسات الحكومية الخاصة ـ في أيامنا هذه - أمراً معتاداً ولا شك أن غياب الالتزام بقواعد الأمن الإلكتروني، مثل وضع مودم غير مخصص للربط بالشبكة العامة، أو مودم غير محمي ضمن الشبكة العامة من شبكات مؤسسة خاصة، مما يتسبب في ثغرات أمنية خطيرة. كما أن تسهيل الأنظمة بوجه خاص في شبكات الاتصالات والطاقة، سمح لمشتركين جدد للدخول بصفة قانونية لشبكات التحكم، التي كانت في الماضي ملكاً خاصاً أو أنها كانت محمية بإتقان. وسواء كان ذلك مقصوداً أو خلاف ذلك؛ فالحقيقة أن أنظمة التحكم في شبكات البنية التحتية أصبحت مفتوحة لدخول أشخاص من خارج المؤسسات المالكة لتلك الأنظمة. لذلك يجب على المصممين أن يعتنوا بكامل المجال، الذي يمكِّن المتسللين والمتطفلين من الوصول إلى أنظمة التحكم الحاسوبي في شبكة البنية التحتية، لأن الممارسين المحتملين لمثل هذا التسلل، بما فيهم إرهابيي الحواسيب والشبكات المتهنين لهذه الأعمال وقراصنة الشبكات، في تزايد مطرد من حيث أعدادهم وأدواتهم التقنية المتطورة. ويلحظ أن هناك تزايداً متسارعاً في المعدات التي يستخدمونها لأغراض الاختراقات والقرصنة، بالإضافة إلى كونهم منظمين، ويتبادلون الأدوات الفنية والتقنيات ومعلومات الثغرات الموجودة في الأنظمة من خلال شبكات الإنترنت بحرية تامة وبالمجان. ولهذا؛ فإنه من الضروري تطبيق إجراءات دقيقة ومدروسة لمجابهة هذه التحديات والتهديدات، مع أن طبيعة الإجراءات المحددة والإجراءات المضادة تجعل تطوير وتطبيق الدفاعات على نطاق واسع في غاية الصعوبة، والأفضل إيجاد دفاع محدد لهجوم محدد، حيث إن مثل هذه الدفاعات تصبح أهدافاً لهجوم مستقبلي، مع العلم أن هناك طرقاً كثيرة للهجوم غير معروفة، وهي في ازدياد مطرد.

وأخيراً؛ فإنه يمكن القول أن شبكات معلومات البنية التحتية تعتمد بطبيعتها على البرمجيات، وضمان اعتمادية أي نظام يعتمد على البرمجيات، يعد من أصعب التحديات الهندسية. كما أن تكاليف نظام فحص شامل لتوثيق قوة الأمان في برمجيات معدة للعمل في بيئة معقدة وآنية، عالية جداً بحيث يصعب تنفيذها، حتى ولو كانت ممكنة من الناحية التقنية. ومما يزيد في تعقيدات هذا التحدي؛ هو حقيقة أن الشركات تتعاقد مع بعضها بصورة متزايدة، وكثيراً ما تكون التعاقدات مع شركات غير محلية بهدف تطوير برمجيات، وهذا النوع من التمويل «Outsourcing» كثيراً ما يؤدي إلى عدم إلمام كامل من قبل المستفيدين من النظام بدقائق المعلومات والأدوات المتعلقة بالأمن الإلكتروني ومستوى التوثيق، التي استخدمها المبرمجون والمصممون. كما أن استخدام البرامج التجارية المتوافرة في الأسواق أمر شائع هذه الأيام، رغم عدم توافر كثير من التصميمات والحقائق في مثل هذه الأنظمة، مما يخل بمستوى اعتماديتها، ويصعِّب الصيانة على المدى البعيد؛ وخاصة عندما تكون هناك حاجة لتغيير الاختيارات المفضلة في اللغة، التي كتب بها البرنامج، بسبب عدم توافر أدوات الإسناد، إما لقدم البرنامج أو توقف إنتاجه.

ويؤدي قدم المعدات أيضاً إلى عدم ملاءمة البرامج الممونة من مصادر خارجية، مما يتسبب في كثير من الأعطال الفنية. وكثيراً ما تضغط المنافسة الشديدة على المطورين لإخراج برامجهم للأسواق قبل إجراء الاختبارات والفحوصات الفنية اللازمة. كما أنه من الممكن تعمد إضافة ترميز خبيث، بقصد ودون علم المشتري أو المالك، في بعض البرامج الحساسة أثناء إنتاجها، مع أخذ الحيطة لضمان عدم اكتشافها أثناء تنصيب البرنامج. بالإضافة إلى ذلك؛ فإن جميع وسائل تحديث ورفع أداء البرمجيات تحتوي على إمكانية إضافة أخطاء رقمية، وإلغاء تصحيحات خوارزمية سابقة، وتغيير تزامن وظائف البرنامج المختلفة، وقد تحدث أخطاء ترميزية «Coding Errors»، وأي من هذه الأمور سيتسبب في زيادة الثغرات الأمنية في النظام. إن وضع وحدة بيانات «نبضة واحدة One Bit» في موقع خاطئ ضمن بنية البيانات أو في خوارزم محكم تقريباً، قد يجعل النظام يعمل معظم الوقت؛ ولكن مجرد تفعيل هذه الوحدة الخاطئة؛ فإن النتيجة ستكون تحولاً من العمل الطبيعي إلى عمل كارثي. إن أنظمة المعلومات، التي أدت إلى مكننة البنية التحتية، معقدة بطبيعتها، والتعقيد نفسه لا يعد مؤشراً حسناً «للاعتمادية». مع أن الإنسان استطاع إيجاد إبداع في غاية التعقيد؛ وفي الوقت نفسه يعد

إلى حد ما عالي الاعتمادية، مثل المكائن النفاثة، والدوائر المجمعة الدقيقة، وناطحات السحاب وغيرها، إلا أن التعقيدات في شبكات المعلومات قد تجعل الشبكة هشة ومعرضة للفشل، مع أنها من المفترض أن تكون مصدراً للقوة. وعلى أية حال؛ فإن هذه الأفكار ليست دقيقة بما فيه الكفاية لاتخاذ قرارات وسياسات هندسية، لأن مدى تأثر الشبكة أو تعرضها لإخفاق شامل لا يحدد إلا بتقديرات دقيقة لعناصر فنية وتشغيلية كثيرة في محيط بيئة تهديدات متكاملة. وفي النهاية؛ فإن أنسب الإجراءات، هو السعي لإدارة المخاطر باعتبار التكاليف، والإنجاز المتوقع، وحجم الاعتمادية التي يمكن فقدانها، مقارنة باحتمالية وقوة التهديدات.

الهجوم التخريبي المتعمد ـ القرصنة الإلكترونية والإرهاب الدولي

لقد أعجبتني مقولة قرأتها منسوبة للعالم «ألبرت آينشتاين» مفادها: (إن الرب حكيم وقادر ولكنه لا يضمر الشر، ولا يمكن أن يقال الشيء نفسه عن الإنسان) وذكرتني هذه المقولة بالآية الكريمة، وهي قول الله تعالى في سورة «النساء الآية ٧٨»: [ما أصابك من حسنة فمن الله وما أصابك من سيئة فمن نفسك]. والذين يحاربون الإرهاب الدولي والقرصنة لابد لهم من فهم كامل تحديات اعتمادية الشبكات، ومن الضروري مراعاة احتمالية الهجوم التخريبي المتعمد. ومع أن الاختراق غير المشروع لأنظمة الحواسيب أصبح حدثاً معتاداً وفي تزايد مستمر؛ إلا أن اقتحامات وتخريب الحواسيب كثيراً ما يقع لشبكات الإنترنت وليس في أنظمة المكننة الآلية للبنية التحتية، وقد يكون هذا صحيحاً الآن، ولكنه قد لا يدوم، وذلك بسبب التزايد المطرد في اندماج الحواسيب الشخصية الخاصة في شبكات البنية التحتية. والواقع أنه كلما زادت الخدمات، التي تتطلب توصيل المستفيدين من الخدمات العامة بشبكات البنية التحتية، سواءً التي تقدمها الدول، مثل خدمات وزارة الداخلية المتعلقة بخدمات المواطنين والمقيمين لتجديد الجوازات ورخص القيادة وإصدار التأشيرات وغير ذلك، أو الخدمات التجارية والبنكية، بما فيها أنظمة البيع والشراء في الأسواق بصورة عامة، وسوق المال على وجه الخصوص، زاد اتصال الحواسيب الشخصية بالشبكة العامة، التي أصبحت جزءاً لا يستهان به في المجتمع المدني.

ومن المؤكد أن الحواسيب الشخصية في هذا العصر أصبحت مكوناً أساسياً من مكونات البنية التحتية. ومع قلة التجارب التاريخية، التي أدت إلى أعطال خطيرة في خدمات البنية

التحتية الناتجة من الهجوم المتعمد على الشبكة؛ فإن متابعة ودراسة تجارب قراصنة الحواسيب، التي تعرضت لها شبكة الإنترنت تفيد كثيراً في إيضاح هذا النوع من التهديدات. وعلى سبيل المثال؛ فقد تم إطلاق فيروس حاسوبي سمي «الدودة Worm» في عام ١٩٨٨م قادر على تكرار نفسه، ومصمم لاستهلاك ذاكرة وموارد الحاسوب، ونتج عنه عطب آلاف الحواسيب قبل أن(تتم السيطرة عليه)، وتلك الحادثة تمثل هجوماً من المستوى الكبير الذي يشمل استحداث برنامج تخريبي قادر على تكرار الاستنساخ الذاتي، وبطبيعته لا يعد مثل هذا النوع من الاقتحام انتقائياً في تأثيراته التخريبية.

وعلى سبيل المثال، ولاستكمال الصورة؛ فإنه يمكن الاستشهاد ببعض حوادث القرصنة الإلكترونية، ومن أهمها: أنه في عام ١٩٩٤م تم تنفيذ أكثر من ١٥٠ اختراقاً لمعامل روما في قوات الجو الأمريكية، حسب نشرات الهيئات الأمنية المتخصصة في الولايات المتحدة[٣٧]، بواسطة اثنين من قراصنة الحواسيب يستخدمون برنامجاً متخصصاً يمكنهم من التنكر كمستخدمين شرعيين. وقد تمكن أولئك المهاجمون من السيطرة على نظام الإسناد للمعمل لعدة أيام، وأنشئوا خلالها، روابط بمواقع إنترنت أجنبية، ونسخوا بيانات حساسة. كما أنهم هاجموا بنجاح أنظمة حكومية أخرى، مثل مقاولي وزارة الدفاع، ومنظمات القطاع الخاص التي لها علاقة بالحكومة. وقد قدرت القوات الجوية، التي لم تكتشف الهجوم إلا بعد ثلاثة أيام، الخسائر الحكومية بـخمس مئة ألف دولار أمريكي، وهذا لا يشمل حساب قيمة المعلومات المسروقة. وهذا النوع من اختراقات القراصنة يصنف بأنه من النوع الذي يستخدم أدوات وأساليب متقدمة للسيطرة على الشبكة، وتنفيذ أعمال تكون في الغالب حصراً على مدراء موثوق فيهم. وهناك سيل من الاختراقات على المواقع الحكومية الأمريكية المتصلة بالإنترنت حدثت عام ١٩٩٦م تعد أمثلة لهذا النوع من الهجوم.

وفي سبتمبر عام ٢٠٠٧م هاجم الطيران الإسرائيلي موقعاً في شمال سوريا على بعد ما يقارب ٧٥ميلاً من الحدود التركية، ادعوا فيما بعد أنه موقع مفاعل نووي تنشؤهُ كوريا الشمالية، واستخدمت إسرائيل في هذا الهجوم الحرب التقنية، واستطاعت تعمية رادارات الدفاع السورية، ودخل سرب من الطائرات وخرج دون أن تراه أو تعترضه وسائل الدفاعات الجوية. والسؤال هنا؛ كيف حصل ذلك؟ والذي يعتقده كثير من المحللين أن عملاء الموساد استطاعوا الوصول لنظام التحكم الحاسوبي في منظومة الدفاع السورية، ووضعوا «حصان

طروادة»، إما بواسطة طائرة بدون طيار اخترقت الأجواء، واستطاعت تحليل الإشارات، ومن ثم أرسلت برنامجاً جزئياً خبيثاً أدى إلى شل فعالية الرادار، أو أنهم وصلوا عن طريق عميل داخل المنظومة، أو أنهم وضعوا البرنامج الخبيث أثناء كتابة البرنامج في روسيا بواسطة عميل يعمل هناك. وليس المهم كيف أوصلوا برنامجهم الخبيث إلى منظومة الدفاع الجوي السورية، ولكن المهم هو أنهم استطاعوا شن حرب الكترونية ناجحة أدت إلى تحقيق أهدافهم وتدمير المبنى الذي اعتقدوا أنه يضم مفاعلاً نووياً.

وفي نوفمبر عام ٢٠٠٩م نشرت شركة «ترند مايكرو» وهي من الشركات المتخصصة في مجال الحماية ومحاربة الفيروسات، إحصائية مفادها أن المملكة العربية السعودية تعرضت لأكثر من ٧٠٠ ألف حالة انهيار في أنظمتها خلال تسعة شهور فقط؛ أي أن المملكة سجلت ٦٤٪ من مجموع الإخفاقات في دول مجلس التعاون لدول الخليج، بينما سجلت دولة الإمارات ٢٠٪ من مجمل الإخفاقات. وأكد التقرير أن أولويات قراصنة المعلومات تتمثل في سرقة البيانات المهمة كالتفاصيل الشخصية، وبيانات بطاقات الائتمان. وتعد دول الخليج ومواطنوها هدفاً مغرياً لهم، ويشكلون خطراً داهماً، في الوقت الذي يصعب فيه مقاضاتهم أو الوصول إليهم لأسباب أهمها وجودهم خارج النطاق الجغرافي لعمليات الاحتيال التي يقومون بها. وقد أقر مجلس الوزراء في المملكة العربية السعودية في ٢٦ مارس ٢٠٠٩م تطبيق نظام مكافحة الجرائم المعلوماتية. وفي هذا النظام تتجاوز مجموع العقوبات المالية مبلغ ١١ مليون ريال، موزعة بالتفاوت المبني على فداحة الجرم الإلكتروني المرتكب. ويهدف هذا النظام للحد من نشوء جرائم المعلوماتية، وتزامن ذلك أيضاً مع إقرار مجلس الوزراء السعودي نظام التعاملات الإلكترونية. ونصت المادة الـ١٤ من نظام جرائم المعلوماتية، على أن تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصاتها تقديم الدعم الفني والمساندة الفنية للجهات المختصة لضبط مراحل هذه الجرائم والتحقيق فيها قبل وأثناء المحاكمة.

ومن المؤكد أن الجريمة الإلكترونية تضاعفت مئات المرات بعد إقبال غير محدود على استخدام الإنترنت، ويعود ذلك إلى حالة أمن المعلومات في المنطقة ونقص برامج التوعية، وعدم وجود تدريب كافٍ للجهات الأمنية. إضافة إلى ذلك، فإن هناك ضعفاً واضحاً في خطوات حماية البنية التحتية للمعلومات في دول الخليج. ورغم ما تزعمه المنظمات الحكومية أن لديها أقوى الأنظمة للأمان ضد الاختراقات؛ إلا أن أبسط الأمثلة على فشل ذلك، هو أن

البنوك وحدها خسرت منذ عام ٢٠٠٨م وحتى نهاية ٢٠١٠م أكثر من بليون دولار من جراء الجريمة المنظمة، حيث تعاني البنوك العربية تحديداً من هجوم اصطياد المعلومات، ويمكن القول أن انتشار المؤسسات المصرفية والوضع الاقتصادي الجيد لدول الخليج قد جعلها هدفاً ممتازاً لقراصنة المعلومات، ويضاف إلى ذلك محاولات غسيل الأموال والبريد المخادع Spam الذي يوهم بالحاجة لنقل المال من دولة إلى أخرى مقابل نسبة خيالية.

وفي عام ١٩٩٦م، تعرض عدد من مقدمي خدمة الإنترنت لهجوم متعمد من مصادر مجهولة تستخدم برامج متقدمة لتحميل مئات الرسائل في الدقيقة في حواسيبها بهدف تعطيلها، واحتوت الرسائل على طلبات للتزامن وعناوين تراسل غير صحيحة، مما أدى إلى إرباك الحواسيب والاستحواذ عليها، وجعلها غير قادرة على تنفيذ التعاملات الحقيقية. ولا تعد هذه الأمثلة شاملة، ولكنها تعطي تصوراً واسعاً عن الهجوم التخريبي، الذي يمكن أن تتعرض له شبكات نقل المعلومات بصورة عامة.

وقد يكون من المفيد استعراض ثلاثة أنواع من الهجوم التخريبي، الذي يؤدي إلى أعطال خطيرة، مثل هجوم هواة قرصنة الحواسيب، وهم المهاجمون الباحثون عن المتعة؛ فرغم عدم دقتهم، إلا أن مجرد اختراقهم للمعلومات سيعرض الشبكة لمشاكل جمة، وخاصة إذا تمكنوا من تغيير البيانات أو تحميل دوائر المدخلات فوق قدرتها أو تسببوا في خفض مستوى التشغيل في الموقع. وفي الغالب؛ فإن دوافعهم تتمحور حول حب الاستطلاع، والتحديات التقنية، والإزعاج، أو بهدف سرقة الخدمة، ولكنهم مع هذا؛ يمكنهم إطلاق حوادث متتالية ينتج عنها خلل واسع الانتشار.

وهناك الفئة الأخرى وهم المهاجمون الفوضويون، الذين يتعمدون مهاجمة عنصر محدد من عناصر التحكم التلقائي الإلكتروني لمساندة أغراض إجرامية أوسع، أو عن طريق عمل عشوائي ليس له هدف واضح أو مقنع سوى التعطيل والتخريب. ومرتكب هذا النوع من الهجوم يهدف إلى التخريب، ولكنه قد يقدِّر أو لا يقدِّر التأثير الحقيقي لفعلته، وغالباً ما يتركز هجومهم على مكونات الشبكات، مثل روابط الاتصالات ونقاط التحكم والمقاسم، حيث يعطلون المعدات؛ إما بتخريب مادي للآلة أو تخريب البرنامج أو البيانات المخزنة. وقد تكون المكونات والعناصر الإلكترونية المعطلة في غاية الأهمية، بحيث يؤدي تعطيل أحدها أو بعضها

إلى توقف النظام، أو أنه يبدأ في إطلاق توقف متتابع ينتج عنة أعطال تسلسلية تؤدي إلى أعطال شاملة على نطاق واسع.

والنوع الأخير والأكثر أهمية: فئة الهجوم المنسق على الشبكة، ومحدثو هذا النوع يتميزون بالتركيز والتنظيم والعمل وفق حسابات دقيقة لتحقيق هدف محدد، وفي الغالب؛ فإن دوافعهم تكون سياسية، وقد يطبقون أفعال المخربين الفوضويين نفسها ولكن بأسلوب دقيق ومنظم، حيث يمكن أن يضعوا «حصان طروادة» أو «قنبلة رقمية» في برنامج التشغيل بغرض التخريب وتعطيل النظام، كما حصل للمفاعل الإيراني عندما تعرض لفيروس «ستكسنت Stuxnet»، وهو قادر على التعرف على شبكة التحكم في منشأة معينة مثل محطة بوشهر النووية ويقوم بتدميرها. ويحمل الفيروس بصمات تكنولوجية لنظام تحكم يسعى للعثور عليه، وهو مجهز للعمل تلقائياً في حال عثر على هدفه، وقد سبق الحديث عنه في الباب الأول. وفي أحياناً كثيرة يستطيع هؤلاء تجنيد متعاونين ممن يعملون في الشبكة المستهدفة الذين يمكنهم استخدام معلوماتهم وصلاحياتهم الشرعية لتنفيذ هجوم على الشبكة وتوقيف شامل للنظام باستخدام وسائل التحكم الإدارية العادية. وليس بالضرورة أن يؤدي الهجوم المنسق على عدد من المكونات والعناصر المهمة أو روابط الاتصالات في النظام إلى تعطيل تسلسلي للأنظمة المستهدفة، إلا أنه قد يؤدي إلى توقف أنظمة التحكم الآلي. وبما أن هذا النوع من الهجوم منسق ومخطط له بعناية؛ فإنه من المحتمل استخدام أدوات تحقق نتائج محددة ومباشرة بدلاً من الاعتماد على ردود الفعل التسلسلية غير متوقعة النتائج.

ويمكن أن يسبب هجوم أي من هذه الفئات الثلاث المستوى نفسه من الأعطال، والاختلاف يكون فقط في الدوافع وطريقة المهاجمين والآلية المسببة للعطل. وعندما يكون نشاط المعرفة وحقولها تحت سيطرة أفراد المجتمع؛ فإن الانتشار الواسع لتقنية المعلومات سيوفر قدرات تخريبية أوسع. وفي الوقت نفسه؛ فإن نمو وتزايد التوصيل والربط بين شبكات الحواسيب يوفر احتمالات إضافية، لما كان في الماضي يعد نظاماً داخلياً مقفلاً، كما أن التقدم المتزايد في أدوات القراصنة وقدراتهم التقنية ينذر بأن أي من هذه الاحتمالات قد يؤدي إلى أخطار واقعية.

الفصل الثالث

الكوارث الطبيعية والأخطاء البشرية
وحوادث أنظمة البنية التحتية
غير المتعمدة

الفصل الثالث

الكوارث الطبيعية والأخطاء البشرية وحوادث أنظمة البنية التحتية غير المتعمدة

عبر السنوات الماضية وقعت كوارث عالمية متعددة تسببت في إخفاقات الشبكة، وظهور مشاكل في البنية التحتية. ففي عام ٢٠٠٣م حصل انقطاع شامل للكهرباء تأثرت منه ١٥ ولاية في الجزء الغربي من الولايات المتحدة الأمريكية[٣٨]، بالإضافة إلى بعض المناطق من كندا والمكسيك. وتضرر نتيجة ذلك الانقطاع في القوة الكهربائية حوالي مليوني نسمة، وتسبب في تأخير الرحلات الجوية، وتوقف القطارات بين دنفر وسان فرانسيسكو. وجرى تتبع سبب الانقطاع، فوجد أنه يعود إلى تحميل يفوق ٥٠٠ كيلو فولت في خط نقل الكهرباء شمال ولاية أوريجان عندما لامس أشجاراً عالية، نتج عن ذلك تكوين دائرة قصيرة منخفضة المقاومة، أدت إلى قفل النظام. وتسبب ذلك في رفع أحمال خطين آخرين بالجهد نفسه وأخرجهما من الخدمة، وفي وقت قصير تبع ذلك خروج شريان القوة الكهربائية بين الشمال الغربي وكاليفورنيا من الخدمة، واستمر الإخفاق في التزايد والنقص متمشياً مع أنظمة الأمان الأوتوماتيكية، التي تحاول موازنة النظام بالتخلص من الأحمال أو زيادتها حسب الحالة دون جدوى، وأدت الحاجة لمزيد من القوة الكهربائية في كاليفورنيا إلى قفل النظام والمولدات في مناطق أخرى تعطلت بسبب القوة الكهربائية العالية المفاجئة، التي لا تستطيع تصريفها. وبعد شهر حصل إخفاق مماثل في المنطقة نفسها.

كما وقعت أعطال متتابعة في شبكة الهاتف الأمريكية المحلية أثرت على ١٦ مليون مشترك في «لوس أنجلوس» و«بليتيمور» و«سان فرانسيسكو» و«بيتزبيرج» في يونيو ويوليو من عام ١٩٩١م، ونسبت إلى أعطال في عدد من الخطوط المتعلقة بأوامر حاسوبية في خوارزم مهم في نظام إشارات التحكم «Signaling system»، واكتشفت الشركة المصنعة أن المشكلة، كانت بسبب تحديث جديد في برامجها لم يوضع تحت الفحص المعتاد لديها؛ علماً أن التغيير كان محصوراً فقط في أسطر قليلة من البرنامج.

وفي سبتمبر عام ١٩٩١م حدث عطل داخلي في القوة الكهربائية في مركز مقاسم هواتف «مانهاتن»، تسبب في قطع نصف المكالمات الدولية في أكبر مقاسم أمريكا لنقل المكالمات الدولية من «نيويورك» وإليها، ونتج عن هذه الحادثة تأثير قوي على التحكم في الملاحة الجوية، لأن المقسم المتأثر يحمل ٩٠٪ من حركة مركز المراقبة الجوية في نيويورك. ورغم عدم وقوع أي حوادث طيران بسبب هذه الأعطال؛ إلا أنه تم إلغاء ٤٠٠ رحلة طيران في ثلاثة مطارات رئيسة في «نيويورك»، وتسبب ذلك في تعطيل عشرات الآلاف من المسافرين لمدة ٨ ساعات، وكان ذلك العطل بسبب فشل مشترك بين أعطال في المعدات وأخطاء بشرية. وبموجب اتفاقية مع شركة الكهرباء المحلية قفلت شركة الهاتف كهرباء المدينة العمومية، واعتمدت على مولداتها الخاصة في أوقات الذروة، مما جعل النظام يعتمد على البطاريات الاحتياطية وسحب مخزونها من الطاقة الكهربائية. وقد اتضح للإدارة حينذاك، أن المشغلين لم يتبعوا الإجراءات المقررة والتأكد من تشغيل سليم للمولدات الاحتياطية، ولسوء الحظ منعت مرشحات الأعطال المولدات من توفير القوة الكهربائية المطلوبة، واعتمدت على البطاريات، مما تسبب في إفراغها من مخزونها. ولم تلاحظ أنظمة الإنذار الصوتية والمرئية لمدة ست ساعات، حتى استهلكت كامل القوة الكهربائية المخزنة في البطاريات الاحتياطية.

وفي يوليو عام ١٩٩٤م جرى تحديث لبرامج الحاسوب الرئيس لتعاملات شركة «ناسدك Nasdaq» الموجود في سوق التعاملات المالية، مما تسبب في تعطيل النظام لمدة ساعتين، نتج عنه خفض حجم المداولات اليومية إلى الثلثين، وتأثر سوق التبادلات المالية ومكاتب المتاجرة ومؤشر السوق في كامل الولايات المتحدة الأمريكية. ويعتمد «ناسدك Nasdaq» على شبكة اتصالات وحواسيب عالمية ومحلية لتنفيذ تبادلاته التجارية في الأسهم، بسبب عدم وجود موقع خاص به، حيث ينفذ الموقع الإلكتروني لناسدك مئات الملايين من عمليات

تبادل الأسهم يومياً، وانتقلت مشكلة البرنامج بصورة مباشرة للحاسب الرئيس «مينفريم، Mainframe» الموجود في «كونيكتيكت Connecticut» والنظام الاحتياطي في «روكفيل Rockville» و«ماريلاند Maryland»، حيث حدَّثت في الوقت نفسه لضمان التوافقية فيما بينها، ففشلت أيضاً.

وتسبب زلزال «نورثريدج Northridge» و«كاليفورنيا» عام ١٩٩٤م في تعطيل المكالمات الهاتفية على مستوى الولايات المتحدة لحوالي مليوني مشترك لمدة ٨ ساعات، بسبب تعطل مقسمين في «شيرمان أو ك Sherman Oak»، وتعطل كذلك حوالي خمسة وثلاثين محطة إعادة للهواتف المتحركة، واستمر عدد من المقاسم في العمل رغم تهدم كثير من مباني المقاسم ومراكز الاتصالات، مما مكن المشتركين الذين لا يستطيعون الاتصال خارج مدينتهم بإجراء مكالمات محلية، وقد استفادت من ذلك منظمات الطوارئ.

وفي يناير عام ١٩٩٠م، حدثت مشكلة محدودة في جهاز توافق في أحد مراكز نظام اتصالات المسافات الطويلة في «نيويورك»، التي تعد أهم مركز لنقل المكالمات بين الولايات المختلفة في أمريكا، وذلك بسبب أداء برنامج التحكم في النظام الذي جرى تحديثه على مستوى عموم الشبكة، إذ أدخل النظام في نمط تجاوز الخطأ المعتاد Fault Recovery Routine، مما نتج عنه توقف معالجة المكالمات الجديدة مؤقتاً، وأدى ذلك إلى منع المقسم من العودة للخدمة ضمن بقية الأنظمة، وتعطلت المقاسم الاحتياطية خلال المعالجة، وتوالت المشكلة في الشبكة، وتتابعت أعطال المقاسم وخروجها من الخدمة، وكانت النتيجة توقف حوالي ٥٠٪ من الحمولة المنقولة على تلك القناة على مستوى الولايات الأمريكية لمدة سبع ساعات. ومن حوالي ١٤٨ مليون محاولة اتصال لم ينجح إلا ٨٣ مليون مكالمة فقط. والمدهش في الموضوع أن الهدف من تحديث البرنامج كان تسريع إعادة معالجة المكالمات بعد أي توقف.

وفي عامي ١٩٦٥م و١٩٧٧م، تعرض الجزء الشمالي الشرقي من أمريكا لعطل كهربائي كبير ومكلف، وفي كلا الحالتين كان سبب العطل تتابع سلسلة من الأحداث نتجت لتطبيق المشغلين ومعدات التحكم التلقائي أساليب التشغيل المقررة التي تعلموها أو برمجت في المعدات عند إيقاف أو فصل المولدات كإجراءات للحماية عند حدوث الحالات غير المعتادة.

وبتحليل دقيق لنماذج الكوارث الطبيعية التي حدثت في الماضي؛ فإنه يمكن القول أن

خدمات المكننة في البنية التحتية في الدول الحديثة تحظى باعتمادية عالية، ففي العقود القلية الماضية كانت الأعطال التي تسببت في التأثير بدرجة كبيرة على معظم المجتمع كانت محدودة جداً، على المستوى الوطني. كما أن الإخفاقات والخروج من الخدمة، التي حدثت بصورة عامة كانت في مجملها انتقائية، بحيث تؤثر على مشتركين محددين أو مقدمي خدمة معينة. وحتى عندما يهدد الخروج من الخدمة سلامة كثير من الناس وأمنهم، كتلك الناتجة من توقف القوة الكهربائية خلال العواصف والحالات الناتجة من قبل خدمات الطوارئ المحلية وبرامج المساعدات الحكومية أثناء الكوارث وفرق الطوارئ العاملة لشركات الخدمات العامة؛ فإن معظم المتخصصين ينظرون لأعطال البنية التحتية على أنها مزعجة وليست كارثة حقيقية. وبجانب شرح نطاق مشاكل الشبكات المتعلقة بالبنية التحتية، تبين الأمثلة المطروحة هنا الأهمية العظمى للترابط المتبادل بين القطاعات المختلفة، مثل قطاعات الاتصالات والطاقة والنقل والاقتصاد؛ فجميعها مرتبطة ببعضها حرفياً ومجازياً؛ وخاصة أنها كثيراً ما تعتمد على الحزمة نفسها من القنوات السلكية واللاسلكية والألياف البصرية.

وأخيراً؛ فإنه من المهم ملاحظة أنه بسبب جميع هذه الحوادث وأمثالها، نفذت في الولايات المتحدة على وجه السرعة أعمال تصحيحية وإجراءات وتغيير في السياسات للمساعدة في تلافيها مستقبلاً، مما يوفر تراكماً في الخبرة يمكن الاستفادة منه في تحسين حماية البنية التحتية مستقبلاً. ويمكن ـ أيضاً ـ الاستفادة منها في بقية بلدان العالم فيما لو قام بعض المهتمين بالأمن الإلكتروني على وجه الخصوص، وأمن البنية التحتية بوجه عام في الدول النامية، التي ليس لديها تجارب كافية، بزيارات منتظمة للجهات المقابلة في أمريكا، وحرصوا على حضور المؤتمرات العالمية ومتابعة الحلول المطروحة. وفي الحقيقة، ليس هناك تأكيدات بأن الأعطال المستقبلية سيكون لها وقع على المواطنين مشابه ومحدد لما حصل في الماضي، إلا أن التجارب الماضية توافر بكل تأكيد رؤية واضحة عن كيفية فشل الشبكات في المستقبل، ومدى إمكانية حصول الفشل. وتبين الأمثلة السابقة أنه في بعض الحالات تفاقمت مشكلة صغيرة مثل كرة الثلج لتسبب إخفاقاً شاملاً، وفي بعض الحالات تسبب عطل عنصر أساسي في النظام في ظهور إخفاق شامل بصورة مباشرة في الخدمة.

إن آلية الأعطال المرتبطة بتتابع ردود الفعل التسلسلية، هي صفة من صفات الأنظمة المعقدة المتوأمة بإحكام مع أنظمة فرعية، وهذه الآلية تعتمد على ميكانيكية النظام نفسه، إذ

إن ما يظهر على أنه حدث غير متسلسل، يحفز أعطالاً متعددة في ما يشبه تساقط قطع لعبة «الضمنة» غير المتوقع. بالإضافة إلى ذلك؛ فإنه يمكن تفاقم المشاكل بسبب الإجراءات المطبقة التي قصد بها الحماية من الأعطال وتوقف النظام. ولمثل هذا النوع من آلية الفشل لا تكون المشكلة الحقيقية هي التي سببت الحادثة، ولكن الذي بدأ المشكلة هو التعامل الخاطئ لأسلوب التشغيل التلقائي في الأنظمة الجزئية. ولا تنتج جميع الأعطال من الاستجابة التسلسلية لخلل طارئ، فالعطل المباشر المستقل لعنصر من عناصر النظام أو لمجموعة من العناصر يمكن أن يتسبب في توقف النظام بالمستوى نفسه. وتعد الكوارث الطبيعية من أكثر المسببات لهذا النوع من الأعطال، لكن العيوب التصميمية في النظام قد يكون لها النتائج الظاهرة نفسها، ويمكن القول ـ وبالنظر إلى أي حادثة محددة ـ أن آلية الأعطال تعتمد على مواصفات النظام وعلى الظروف المتوافرة للحادثة، وتوضح الآليات العريضة المشروحة هنا أقصى التصورات. وفي الحياة الحقيقية، فإن كثيراً من الأعطال تحتوي على بعض الخواص من هذين المحورين، وتقع بينهما.

الأعمال الإرهابية وتأثيراتها على البنية التحتية والاقتصاد والسياسة

في عام ٢٠٠٦م[٣٦] وقع تفجير أنبوبين متجاورين في موقع جبلي جنوب روسيا، وكان هذان الأنبوبان يحملان الغاز الطبيعي لدولة جورجيا، والأنبوبان جزء من شبكة التغذية العامة للغاز. وقد استغرق وقت تنفيذ العملية عدة ساعات، بسبب أن الأنبوبين الأساسي والاحتياطي متجاوران ولا يفصلهما سوى نهر صغير، وبالتزامن مع هذا العمل الإجرامي نفذ هجوم مماثل على برج الضغط العالي، الذي يحمل الكهرباء إلى جورجيا من روسيا، وفي غضون دقائق أصبحت جورجيا بدون غاز أو كهرباء. وبتوافر احتياطي يكفي فقط لمدة ٢٤ ساعة عاشت جورجيا في عصور ما قبل الثورة الصناعية لمدة أسبوع رغم الضغوط الكبيرة التي مارستها الحكومة المحرَجَة على الممولين الروس لإعادة الخدمة.

ومما يثير القلق هذه الأيام؛ أن الإرهابيين قد تعلموا استراتيجيات وطرقاً فعالة لمحاربة الدول النظامية، دون الحاجة لامتلاك أسلحة الدمار الشامل، وهي «تخريب أنظمة البنية التحتية»، وذلك إما باستخدام الحرب الإلكترونية كما حصل في «أستونيا» عام ٢٠٠٧م، عندما وقع الصدام بين المواطنين من أصل روسي والمواطنين الأصليين، بسبب إزالة نصب

الجندي المجهول الروسي، وتطور النزاع بين الفئتين ليدخل في الصراع الإلكتروني، وذلك كون «أستونيا» أحد أكثر الدول المعتمدة على استخدام الشبكات، التي تحظى بأكثر نفاذ إلكتروني من خلال شبكات الإنترنت. أدى ذلك إلى إغراق الحواسيب، التي تدعم معظم المواقع المستخدمة بشكل مفاجئ بطلبات وهمية أدت إلى تعطيل بعضها، بسبب الأحمال المتزايدة، والبعض الآخر توقف بسبب الاستفسارات الواردة للتأكد من عملها، ونتيجة لهذا الهجوم توقفت الاتصالات بين البنوك وبين أجهزة الصرف الآلي، وكذلك الصحف الإلكترونية ومواقع الدولة الإلكترونية. لقد تعرضت «أستونيا» لما يعرف بهجوم منع الخدمة الرقمية DDOS، وهو إغراق الإنترنت بحركة مرور إلكترونية مصممة لتعطيل النظام وإيقافه. وقد اتهمت «أستونيا» المخابرات الروسية بهذا الإغراق، ولكن الروس ادعوا أن من قام به هم المتطرفون في «أستونيا»، أو أنه نتج عن تفجيرات وتخريب بهدف تحقيق خسائر اقتصادية للدول المستهدفة. وكما سبق ذكره فإن معظم شبكات البنية التحتية مهيأة لمقاومة الأضرار العشوائية؛ لأنها مصممة لمقاومة الكوارث الطبيعية، أو الانقطاع الناتج من الإنشاءات. ويتطلب الأمر لتنفيذ عمل إرهابي مؤثر، معرفة قدر كبير من علم الشبكات، إما بالدراسة الأكاديمية أو عن طريق المحاولة والخطأ، وبالإمكان شل شبكات البنية التحتية بشمولية مخيفة بكل سهولة عن طريق اختيار النقطة الصحيحة. ومجرد معرفة علوم الشبكات وفهمها ليس كافياً، فالهجوم الناجع يتطلب معرفة دقيقة ومحددة للموقع الصحيح الذي يجب أن تسدد إليه الضربة. وهذا الموقع الذي أطلق عليه مسمى «الموقع القاتل للشبكة»، يمثل أهم نقاط النظام التي تتعامل مع معظم أوامر الشبكة وتتحكم في تشغيلها وتوزيع الأحمال، والتي يمكن أن تشل كامل الشبكة المستهدفة عند تخريبها.

ومن أهم القضايا، التي يهتم بها الإرهاب الدولي ويحرص على جمع معلومات دقيقة عنها، قضية: «الموقع القاتل للشبكة»، وهي نقطة في نظام البنية التحتية يؤدي تخريبها إلى تعطيل شامل وكلي في الشبكة المستهدفة، أو أنها تؤثر بصورة كبيرة على الأسواق الاقتصادية والقطاع المالي؛ كما حصل في تفجيرات ٩/ ١١، وعادةً ما يتم تحديدها من قبل مجاميع سرية تعمل في المنطقة المستهدفة. ويهدف المهاجمون بهذا العمل إلى زعزعة الثقة في السوق لتحقيق انخفاض في قدرات السوق وحصول فوضى سوقية مؤثرة. والمزعج في هذا الإطار أن الإرهابيين يتعلمون بسرعة ملحوظة عن كيفية اكتشاف «الموقع القاتل للشبكة» ويخططون لمهاجمته. وتعلمت

المنظمات الإرهابية دروساً جمة من تجارب الدول النظامية، مثل الولايات المتحدة وإسرائيل، اللتان تبدآن حروبهما بتدمير شامل لجميع مكونات البنية التحتية للعدو، كما حدث في العراق، وأفغانستان، وغزة، وجنوب لبنان، فضلاً عما تعلمه الإرهابيون من التجارب التي خاضوها، أن مهاجمة البنية التحتية وأنظمة الاقتصاد الأساسية تحقق ناتجاً ربحياً يساوي أضعاف ما تم إنفاقه لتنفيذ الهجوم. ويتّبع الإرهابيون طرقاً متعددة لتعطيل الشبكات، مثل اختيار موقع له قيمة اقتصادية عالية ومحاولة تفجيره كآبار وخزانات البترول، أو محطات الطاقة الكهربائية أو النووية، مع أن هذا ليس من السهل تحقيقه، لأن مثل هذه المواقع تكون في الغالب تحت حماية مكثفة. ومن ذلك، على سبيل المثال، أن القاعدة حاولت تنفيذ هجوم مباشر على أحد أهم مصادر البترول في رأس تنوره بالمملكة العربية السعودية في عام ٢٠٠٦م، ولم يتمكن المجرمون من اختراق الطوق الأمني الثاني، لذلك توجه الإرهاب إلى أسلوب التخريب الذي ينتج عنه تعطيل تسلسلي، كما تم شرحه فيما سبق.

التأثير الاقتصادي الناتج من مهاجمة «الموقع القاتل للشبكة»:

عندما انخفض مستوى القوة الكهربائية في أجزاء من ولاية «أوهايو» في أمريكا إلى أقل من الهامش المقرر في ١٤ أغسطس عام ٢٠٠٣م، وذلك بسبب بعض الأخطاء البشرية والفنية، أدى ذلك إلى إعادة توزيع للأحمال نتج عنه أعطال تسلسلية أدت إلى توقيف مئات المولدات، وانتشرت الأعطال في كامل الشمال الشرقي في أمريكا بما في ذلك أجزاء من كندا. وما كانت بدايته مجرد تأرجح هيِّن في مستوى التيار الكهربائي في شبكة الطاقة الكهربائية للولاية، تحول في وقت قصير إلى حرمان ما يقارب خمسين مليون نسمة من الكهرباء. وفور حصول ذلك، اتجهت أصابع الاتهام للإرهاب الدولي، ورغم أن الإرهاب بريء من ذلك؛ إلا أنه كان ولازال محتملاً.

ولتوضيح مدى خطورة هذا النوع من الأعطال التسلسلية، سواء الناتجة بأخطاء مماثلة أو بأفعال إرهابية؛ فإنه يمكن العودة إلى تقرير «التأثير الاقتصادي لأعطال الطاقة الكهربائية الشاملة في أغسطس ٢٠٠٣م The economic Impacts of the August 2003 Blackout» الذي أعده مجلس موارد المستهلك للكهرباء «Prepared by the Electricity Consumers Resource Council (ELCON) - February 9. 2004». وبالرجوع لتقديرات «مجموعة

أندرسون الاقتصادية (Anderson Economic Group (AEG» التي قدرت التكلفة الإجمالية المحتملة بمبلغ يتراوح بين ٤,٥ و٨,٢ بليون دولار أمريكي وهذا المبلغ يشمل ٤,٢ بليون دولار خسارة في دخول الموظفين والمستثمرين، و١٥ مليون دولار إلى ١٠٠ مليون دولار تكاليف إضافية على الحكومة، وبليون إلى بليونين تكاليف المرافق المتأثرة، و٣٨٠ إلى ٩٤٠ مليون دولار تكاليف مرتبطة بأضرار لحقت بالأصول الثابتة. وكما هو واضح من هذه التقارير التحليلية؛ فإن الخسائر باهضة للغاية، وتصبح أكثر إزعاجاً لو قورنت بالتكلفة الإجمالية، التي سيتكبدها الإرهابيون لتحقيق هذا المستوى من الدمار المادي والاقتصادي. وبدراسة التقارير التي نشرت بعد كارثة ١١ سبتمبر ٢٠٠١م، قدرت تكاليف تجهيز وتدريب فريق انتحاري لعدة سنوات للقيام بمهمة كمهمة ٩/ ١١ بحوالي خمس مئة ألف دولار أمريكي، نتج عنها خسائر مادية واقتصادية تجاوزت ٨٠ بليون دولار، أي بعائد ربحي في صالح الإرهابيين يصل إلى ١٦ ألف ضعف التكاليف المادية المستثمرة، أما الخسائر البشرية فهي حوالي ١٩ إرهابي مقابل أكثر من ثلاثة آلاف ضحية.

أنواع التخريب الإرهابي:

إن أنواع التخريب الإرهابي لا يمكن حصرها بدقة، غير أنه يمكن إيضاح أهمها فيما يلي:

التعطيل الشامل للأنظمة Systems Disruption :

وهي طرق يسيرة لمهاجمة الشبكات المهمة في البنية التحتية، التي تمثل الحياة الحديثة في العالم، مثل شبكات الكهرباء، وأنابيب نقل البترول والغاز، وشبكات توزيع المياه، وشبكات الاتصالات، وشبكات الطرق والمواصلات. ويهدف الهجوم ليحقق تآكل شرعية الدولة المستهدفة، ودفعها نحو الفشل، وذلك بشل أو توقيف خدماتها الضرورية لمواطنيها، ومنعها من السيطرة على المجتمع، وإضعاف قوتها الدفاعية. وعند تطبيق استراتيجية تعطيل الأنظمة على شبكات الكهرباء أو أنابيب نقل البترول في أي بلد من بلدان العالم، مثل أمريكا أو المملكة العربية السعودية أو روسيا أو دول أوروبا، سيظهر بوضوح بداية فوضى اقتصادية غير مسبوقة، وسينتج عنها عدم توازن في اقتصاد البلد المستهدف يؤدي إلى الأسوأ. ولتوضيح ذلك؛ فإنه

يمكن النظر في بعض الأرقام، التي نتجت من تعطيل البنية التحتية في العراق من قبل القوات الأمريكية، حيث فقدت حكومة العراق ما يقدر بخمس مئة مليون دولار أمريكي من عوائد البترول، بسبب الهجوم على أنبوب نقل البترول في جنوب شرق العراق، بتكلفة تقدر بألفي دولار أمريكي فقط؛ أي بعوائد استثمارية تقدر بـ ٢٥ مليون في المائة (٢٥,٠٠٠,٠٠٠٪)

تخريب الشبكات النشطة (Dynamic Networks) والأعطال التسلسلية:

إن الصورة الحقيقية لعمل شبكات البنية التحتية ليست انعكاساً لمعمارية ربط الشبكات الساكنة، لأن البنية التحتية تتكون من شبكات متحركة، أي «ديناميكية» تتدفق من خلالها المعلومات والبيانات والطاقة والمواد بصورة متغيرة ودائمة ومنتظمة، وهذه الديناميكية تؤدي إلى خلق مجموعة جديدة من الثغرات الأمنية، التي يمكن استغلالها من قبل المنظمات الإرهابية العالمية، وتحصل هذه الأعطال التسلسلية في الشبكات الديناميكية، حتى لو كان العطل في إحدى الطرفيات المنفردة ذات التحميل العالي، وذلك على النحو التالي:

- عند تعطل النهاية الطرفية، بسبب حادث عرضي أو هجوم متعمد، يتم تلقائياً إعادة توزيع الأحمال، التي تتعامل معها تلك الطرفية بسرعة على بقية النهايات الطرفية في الشبكة.

- عند عزل أي نهاية طرفية ذات أحمال عالية من الشبكة، فإن أحمالها توزع على بقية أجزاء الشبكة، وهذه الزيادة في تدفق المعلومات تؤدي إلى إغراق النهايات الطرفية، التي لا تتمتع بقدرات عالية. ولحماية مثل هذه الطرفيات؛ فإن معظم الأنظمة تخرج النهاية الطرفية من الخدمة بصورة تلقائية بعد توزيع أحمالها، مما ينتج عنه أعطال تسلسلية في بقية أجزاء الشبكة حتى تصل إلى توقف تام وشامل، لأن كل عطل يؤدي إلى توزيع أحمال المحطة المتعطلة على بقية أجزاء الشبكة.

- أن الأعطال التسلسلية لا تحدث غالباً إلا في الشبكات غير المتجانسة، التي تتألف من نهايات طرفية قليلة بسعات أحمال عالية، في حين تكون باقي النهايات ذات سعات منخفضة. أما الشبكات المتجانسة، التي يتساوى فيها توزيع الأحمال بين نهاياتها الطرفية؛ فإنها لا تعاني من الفشل التسلسلي، ولكن لسوء الحظ، فإن جميع شبكات البنية التحتية غير متجانسة حسب التصاميم.

الباب الثالث

الفصل الأول

سبل حماية البنية التحتية ورفع مستوى أمن العمليات

الفصل الأول

سبل حماية البنية التحتية ورفع مستوى أمن العمليات

الذين يهوون لعبة الشطرنج لابد أنهم شاهدوا شخصين يتنافسان في اللعبة، ولاحظوا إمكانية إنهاء اللعبة خلال خطوة أو خطوتين، كما قد يلحظون تحركاً من الجهة الأخرى يمكّن المتنافس الآخر من تلافى الخطر، ولكن؛ لا أحد من المتنافسين قد تنبه لذلك، والسبب أن المراقب من خارج المنافسة يرى بوضوح أكثر ممن هو في داخلها. ولأنني متيقن من دقة هذه المقولة؛ فإنني استخدمها دوماً عندما أسمع أو أقرأ سرداً للمشاكل أو العيوب دون أن يتبرع أو يحاول مَنْ سردها أن يضع اقتراحات وحلولاً لها، وكان ردة الفعل على الدوام ليس المهم التشخيص والتنظير، لكن المهم رؤية الحلول ووسائل تلافيه. لذا فإن البحث عن الحلول ضرورياً وملزماً.

قبل البدء في وضع الحلول والمقترحات لحماية البنية التحتية والمحافظة على إنجازات الحضارة؛ من الضرورة بمكان معرفة المستوى، الذي عند بلوغه يتحقق رفع درجة اعتمادية البنية التحتية لدرجة عالية يقبلها المجتمع. ولا يمكن تحديد المستوى المقبول إلا بتوعية كامل المجتمع من خلال عقد المؤتمرات والورش العلمية لمناقشة موضوع الاعتمادية. ولن يكون الأمر سهلاً ما لم يحدد معنى الاعتمادية دون أي لبس، وتحقيق الفهم التام لأنواع الاعتمادية وأشكالها المتعددة، التي سيأتي ذكرها. فالنوع الأول من الاعتمادية، هو أن يعتمد شيء أو كائن على شيء آخر بحيث لا يستطيع أي منهما البقاء دون الآخر. ولتوضيح ذلك، فسنفترض أن

رجلين يمسكان بطرفي حبل، وأنهما يقفان على سطح مستوٍ ولكنهما يميلان بعيداً عن بعضهما بزاوية أكثر من ٣٠ درجة، أي أن قدميهما أقرب لبعضهما من رأسيهما، ولو تصورنا أن أحدهما ترك الحبل، أو أن الحبل لم يستطع مقاومة الشد فقطع، فالنتيجة أن كلا منهما سيسقط أرضاً. ولو شيد بناءين بدلاً من الرجلين، وجعلنا كلاً منهما يدعم الآخر بالطريقة نفسها، فسنحصل على النتيجة نفسها وينهار البناءان، وهنا يمكن القول أن هناك اعتمادية تبادلية بين البناءين، وهذا النوع من الاعتمادية يعد اعتمادية هشة، وهو يمثل العلاقة بين مجتمعاتنا المتحضرة والبنية التحتية، حيث إن انهيار إحداهما يؤدي بالضرورة إلى انهيار الأخرى. وأقرب مثال على ذلك ما حصل في جورجيا عام ٢٠٠٦م حينما توقفت جميع وسائل الحياة الحديثة وعاشت البلاد في عصر ما قبل الثورة الصناعية، عندما فجرت مصادر الغاز ومحطات الكهرباء في اليوم نفسه[٢٨]. أما النوع الثاني من الاعتمادية، فهو عندما يكون البناء أو الشبكة مترابطة من عدة محاور، ولتسهيل فهم هذا النوع من الاعتمادية، فإنه يمكن النظر في شبكة مرمى كرة القدم، ولكنها مصنوعة من حلقات مثل حلقات السلاسل المعروفة، فسنجد أن تلف حلقة واحدة من السلسلة لا يؤدي إلى إفساد الشبكة، بل إنها ستصمد وتؤدي عملها دون أي إشكال، كما يمكن إصلاح الحلقة المقطوعة وإعادة الشبكة إلى ما كانت عليه. وهذا النوع يعد اعتمادية صلبة، بحيث لا يتسبب تعطيل أي عنصر من عناصر النظام في إسقاط كامل النظام ولا يوقف تشغيله.

ومن البديهي لتحقيق أساس متين لأمن فاعل بكفاءة عالية؛ فإنه يجب وضع استراتيجية شاملة لأمن البنية التحتية، بحيث تطبق هذه الاستراتيجية كلما دعت الحاجة إليها بتكلفة منخفضة. وفي أنظمة معقدة ومتشابكة مثل البنية التحتية، فإنه لا يمكن وضع استراتيجية فاعلة إلا بالتعاون الوثيق بين الدولة والقطاع الخاص وجميع فئات المجتمع وعناصره. فالحلول الناجعة لأمن البنية التحتية تعد أساساً لبنية تحتية آمنه وذات اعتمادية عالية يمكن قبولها، ولا يمكن تحقيقها دون قرار سياسي واجتماعي وتشكيل لجان متخصصة لجمع عناصرها ومكوناتها وصياغتها على هيئة قوانين وتعليمات وسياسات. ثم يأتي بعد ذلك عقد الندوات وورش العمل، التي ترفع مستوى الوعي الأمني لدى كامل فئات المجتمع، لتحديد المستوى المقبول للاعتمادية. ومن أهم العناصر التي تحقق أمن البنية التحتية، الإنفاق السخي على تطويرها وصيانتها. وبالرجوع إلى دراسة قدمت في منتدى الرياض الاقتصادي المنعقد في

ديسمبر ٢٠٠٤م[٣٩]، يتضح أن الإنفاق على البنية التحتية في المملكة العربية السعودية، تدنى في السنوات الماضية بشكل ملحوظ. فبينما كانت له الأولوية في الخطط التنموية الأولى والثانية والثالثة بمعدل ٤١,٣٠٪ ، و ٤٩,٣٠٪، و ٤١,٣٠٪، من إجمالي الإنفاق على التوالي، إلا أن نسبة الإنفاق انخفضت اعتبارًا من خطة التنمية الرابعة، حيث تدنت من ٢٨,٩٠٪ إلى ٢١,٨٠٪ في الخطة الخامسة ثم إلى ١٦,٢٠٪ في الخطة السادسة و أخيراً إلى ١٢,٧٠٪ في الخطة السابعة، لذا؛ فإنه من الطبيعي أن تنعكس قلة الإنفاق على البنية التحتية، سلباً على بقية القطاعات الاقتصادية والصناعية والزراعية والسياحية والخدمية وغيرها من القطاعات. وبالعكس تماماً؛ فإن زيادة الإنفاق على البنية التحتية ستؤدي بكل تأكيد إلى توسيع القاعدة الاقتصادية، مما يشجع على جذب الاستثمارات المحلية والأجنبية، وتشغيل العمالة الوطنية، وخفض الهجرة من الريف إلى المدن .

ويعد رفع مستوى الأمان والاعتمادية في البنية التحتية، من الركائز الأساسية لأمن وسلامة أعمال المؤسسات الخاصة والعامة ، فهي تحقق الاستراتيجية الخصوصية، وتخفف من مخاطر حجم العمليات وتوافقها مع الأنظمة التشريعية، لأن البنية التحتية التي تتمتع بمستوى أعلى من الأمن والسلامة، تغرس ثقة أكبر في الدولة والمؤسسات الخاصة والعامة، والخدمات التي تقدمها تلك المؤسسات، والثقة في أن المجتمع ومؤسساته يحظى بحماية عالية، وأن خطوط الإنتاج من قبل مقدمي الخدمات والممونين والمستفيدين آمنة وفاعلة. وعندما يكون أمن البنية التحتية محكماً وخاضعاً لقوانين وتشريعات تحدد تحركه وتتحكم في سير عناصره بوضوح، فقد يظن البعض أن مثل هذه الإجراءات تعيق وصول المنتجات والخدمات إلى الأسواق في الوقت المناسب، لكنه من المؤكد أن التشريعات الواضحة تدعم حركة السوق. فتأثير الحوادث الأمنية على التقدير العام للمخاطر المتعلقة بالبنية التحتية وخفض الإنتاجية واضح للجميع، لكن الغموض يقع في معرفة عدد مكررات تعامل المؤسسات الحكومية والخاصة مع قضايا الأمن والسلامة، أي تكرار الإجراءات التي تطبقها المؤسسات الحكومية والخاصة لمحاولة إيجاد بنية تحتية مأمونة واستراتيجية واضحة لإدارة الأزمات والكوارث، بهدف تحقيق عمليات تشغيلية آمنة. فعدم توفر خطة قياسية متكاملة يتم تطبيقها عند ظهور أي مخاطر أمنية، سيؤدي إلى تقييم المخاطر وفق مبدأ كل حالة بانفراد عند حدوثها، مما يزيد التكاليف، ويتسبب في فوضى تؤدى إلى فشل في إدارة الأزمة بصورة سلسة وناجعة. والسبب في ذلك أن أمن وسلامة البنية

التحتية ليس مجرد حدث عابر ينبغي معالجته عند حصوله؛ بل أنه أمر ضروري يجب الاهتمام به بأسرع وقت، والاستعداد له قبل حصوله وبشمولية تامة. وتتطلب دراسة وضع الحلول لحماية البنية التحتية من الأعطال الكوارثية النظر في عدد من المحاور، التي يحتمل أن تؤدي إلى تعطيل شامل ينعكس على الأداء السليم للنظام، الذي سيؤثر بدوره على المصالح الوطنية بصورة عامه، والتي يلزم جمعها وتبويبها والعمل على تطبيقها من قبل لجان متخصصة، وتشمل:

١- المحور الفني.

٢- المحور التشغيلي.

٣- المحور البشرى.

٤- محور القرصنة الإلكترونية والإرهاب.

٥- المحور الإعلامي.

وسيتم مناقشة كل محور على حدة في الفصل الثاني.

الفصل الثاني

المحاور الأساسية لحماية البيئة التحتية

الفصل الثاني

المحاور الأساسية لحماية البيئة التحتية

(١) المحور الفني:

يعد قطاع شبكات المعلومات عنصراً مشتركاً لجميع أجزاء البنية التحتية، لذا فإن هذه الشبكة تمثل الجزء المهم الذي يجب الاهتمام باعتماديته وأمنه، ابتداءً من مرحلة التصاميم الهندسية والإنشائية، ووصولاً إلى تصنيف اعتمادية شبكات الاتصالات ونقل المعلومات، وتطوير تصور كامل لمكامن قوتها وضعفها. ويتكون هذا القطاع من حلقات تسلسلية تعتمد كل حلقة منها بأسلوب تبادلي مع عدد من الحلقات الأخرى، لذلك ترتبط اعتمادية كامل الشبكة بقرارات التشغيل قبل عمل الشبكة وأثناء تصاميمها الهندسية. ومن الضروري الأخذ بعدد من الاعتبارات، وذلك على النحو التالي:

اعتبارات الإنشاء والتصميم:

يمكن نظرياً تصميم شبكة معلومات صحيحة باعتمادية عالية، وجعلها تعمل بصورة سليمة من الوهلة الأولى، ولكن الشبكات تتغير وتتطور وتنمو بصورة مستمرة مع مرور الوقت وتقدم التقنية، بالتراكم والإضافات وتغيير وظائفها بالزيادة والنقص، كما أن متطلبات الأسواق هي الأخرى تنمو باستمرار وتسارع. وفي مثل هذه البيئة المتغيرة، لا يمكن أن يستمر التصميم ثابتاً طوال الزمن، لذا فإنه ـ ولسوء الحظ ـ لا توجد شبكات كاملة ومثالية، ودائماً

يوجد حاجة لحلول هندسية جديدة لمشاكل طارئة أو جديدة. وبناء عليه؛ فإنه من الضروري أثناء تصميم الشبكة، النظر بعمق في أنماط وطرق التراسل، حيث أن مستويات الإشارات ذات الاهتمام تتدرج من إشارات تناظرية Analog تنقل على دوائر مخصصة، إلى أنماط رقمية معقدة تجمع وتنقل على قنوات بيانات عريضة، بما في ذلك قنوات الألياف البصرية والكوابل المحورية والأقمار الصناعية. ويمكن أن تكون هذه الإشارات مشفرة أو غير مشفرة، وقد تكون هدفاً للاعتراض والمراقبة والتشويش، ولكن بدرجات متفاوتة. وعند اختيار واعتماد التصميم؛ فإنه يجب تحديد نقاط الضعف، التي قد تؤدي إلى الأعطال المادية والإلكترونية، فالتحديات التي تواجه خبراء بناء وتصميم الشبكات ذات الاعتمادية العالية لا تخفى على أي متخصص، لأن أسباب الأعطال تغطي كامل المجال من العوامل الطبيعية إلى الطبيعة البشرية، ومن الحوادث الطبيعية إلى أفعال عدائية من أشخاص أو هيئات. كما أن آليات الأعطال تختلف من نظام لآخر؛ فالأنظمة المترابطة بإحكام، غالباً ما تتعرض للأعطال الشاملة بسبب أعطال متتابعة في نظام فرعي يتسبب في تعطيل أنظمة فرعية أخرى مرتبطة به على هيئة متتاليات تؤدي إلى فشل شامل للنظام. وفي حالات أخرى يكون العطل الشامل بسبب تعطل عنصر أو مكون حرج من عناصر ومكونات النظام.

ومن الضروري اتباع عدد من الإجراءات عند الشروع في تصميم الشبكات لتحقيق الاعتمادية، وأولها وأهمها: العمل الجاد على تخفيض احتمالية تكرار الأعطال وتوقف النظام، وذلك لتقليل الحاجة للدفاع عن أمن وأمان الشبكة، وهو مبدأ في غاية الأهمية أثناء التصاميم الأولية. ومن الضروري ـ أيضاً ـ التركيز على مميزات النظام الخارجية والثابتة في التصميم، واقتراح استراتيجيات تهدف لتقليص احتمالية فشل العناصر والمكونات الفرعية للنظام، مثل التحكم في بيئة النظام، وتأهيل العناصر والمكونات بدقة، وتحقيق أمن إنشائي وإلكتروني وبرمجي في الشبكات، وإجراءات وتدريبات شخصية للمشغلين وبقية أطقم العمل، وكذلك تحديد واحتواء وتجنب نقاط الضعف وفشل النقاط الطرفية المعزولة. ويأتي بعد ذلك موضوع النظر في مسألة التقليل من تأثير الأعطال، التي أثبتت التجارب الماضية أن حدوثها يتكرر، ويتم ذلك من خلال التركيز على تعامل الأجزاء الفرعية وتأثيراتها على بعضها، ومعرفة أنواع أعطال تلك الأجزاء، وكشف الانحرافات التشغيلية، التي تنتج من تلك الأعطال، وتحديد ردود فعل النظام عند انخفاض أداء أحد عناصره.

ومن المهم ـ أيضاً ـ العودة للتجارب التشغيلية السابقة، في الأنظمة المشابهة للاستفادة منها، لأنها تقدم منظوراً مفيداً للتصميم. ولا يمكن التركيز بما فيه الكفاية على مبادئ التصاميم التي تؤدي لاسترجاع عمل النظام عندما يتعرض للأعطال، (أي الحرص على تحقيق متوسط منخفض لمدة إعادة النظام لحالته الطبيعية بعد التوقف)، وكذلك إعادة تنشيط دورة عمل المعدات، والتدخل البشري بعد حدوث توقف النظام، وخاصة عندما يكون نظام الطوارئ أو النظام البديل غير كافٍ، أو أصبح غير ذي جدوى، اذ أن إمكانية الاسترجاع الطبيعي والسريع للنظام، يمكن تحديدها نظرياً أثناء التصاميم من التجارب السابقة، إلا أن هذا يتطلب اهتماماً جماعياً في جميع المراحل أثناء التصاميم الهندسية.

وتمثل عمليات استرجاع تشغيل النظام أكبر مطلب للتطوير، والتحديث، ومن المهم التنبؤ بالمتطلبات، التي تفرضها الخواص التصميمية، والخصائص التي ليس لها تأثير على كمال التصميم، ولكن لها تأثير مهم عند إعادة تشغيل وتهيئة النظام. ولتوضيح ذلك؛ فإنه يمكن استرجاع ما حصل بعد كارثة عام ١٩٦٥م فعندما تعطلت كهرباء «نورث إيست Northeast»، تحركت السفينة البحرية الأمريكية «USS Bristol» من «بروكلن» ووفرت الطاقة الكهربائية لأحد محطات الكهرباء المدنية. ومن تلك الحادثة يمكن أن يفكر المهندسون في وضع وسائل لتوصيل محطة توليد الطاقة في سفن لمحطة ساحلية أو قريبة من الساحل، وتجهيزها بمداخل للكهرباء المنقولة من السفن، والبدائل كثيرة إذا ما اعتمدت وتم التفكير فيها أثناء التصاميم. وقد يكون من المناسب زيادة هامش التعامل بين الأنظمة الفرعية أثناء مراحل التصميم، وذلك لتقليص الأعطال التسلسلية عن طريق تقليص احتمالات فشل التعامل فيما بينها. وقد يكون من المفيد ـ أيضاً ـ اتخاذ إجراءات: مثل توزيع جغرافي للعناصر الأساسية للنظام بهدف تخفيض احتمال حدوث أعطال مستقلة تؤدي إلى توقيف شامل للشبكة، وإضافة بدائل وتكرار للمعدات، وتنويع البرامج التشغيلية. كما أن تحسين أمن المنشآت أو تقوية الحواجز لمقاومة الاختراقات يسهم في منع الأعطال الناتجة من الهجوم المتعمد، أو تقليل آثاره.

وعند اختيار الاستراتيجيات والبرامج أثناء التصميم؛ فإنه يجب ملاحظة أن كثيراً من الاستراتيجيات المفيدة لنظام فرعي مستقل، قد تتعارض مع تصاميم نظام فرعي آخر، ومع أهداف أداء الشبكة. وكمثال؛ فإنه يمكن أن يؤدي تنويع البرمجيات عن طريق توظيف أنظمة فرعية تعمل ببرامج تشغيلية مختلفة، إلى تلافي أعطال نقطة منعزلة، ولكنها قد تؤدي إلى رفع

ملحوظ للتكاليف وتأثير سلبي على الأداء، بالإضافة إلى أن مميزات الحماية المضافة بحسن نية قد تسبب ثغرات أمنية إضافية وأعطال بأشكال جديدة. وللتوضيح؛ فإنه يمكن أخذ مثال آخر للتدليل على زيادة العناصر بهدف التبادلية، ومع أن تطبيق هذه الاستراتيجية يهدف إلى تقليص أثر الأعطال المحصورة في العنصر المكرر؛ إلا أنها قد تكون ضارة في سيناريو آخر، لأنها تزيد تعاملات النظام الفرعي وتخلق مسارات يمكن أن تؤدي إلى انتشار العطل خارج ذلك النظام الفرعي. كما أن إضافة عنصر زائد أو مكرر قد يؤدي إلى إيجاد بدائل أكثر للمخترقين، مما يفاقم التخوف من ضعف أمن الشبكة.

والمهم هنا معرفة أن أي استراتيجية عندما تطبق بصورة منعزلة، قد تخفض الاعتمادية الكلية للشبكة بدلاً من دعمها، كما هو الحال في الوصفات الطبية، حيث إن علاجاً محدداً قد ينفع لمرض، ولكن إضافة نوع آخر قد يؤدي إلى مضاعفات أخرى. وبكل وضوح؛ فإنه قد يكون من الضروري تطبيق منهجية مبنية على مبدأ الترابط بين الشبكات، رغم أنها تؤدي لبعض المقايضة والتضحية بخاصية أو بوظيفة أخرى. والمهم أثناء التصميم أن تؤخذ أمور موازنة التكلفة، والأداء، وتأثير اعتمادية البدائل الفنية بعين الاعتبار، في إطار احتمالية حدوث التهديد، وحجم الضرر المتوقع عند حدوثه. ومن الضروري ـ أيضاً ـ الإجابة عن عدد من الأسئلة عند دراسة المقايضة مثل: هل سيعمل الحل المطروح؟ هل يمكن تطبيقه؟ ما هو تأثير الحل على احتياجات المجتمع والأسواق؟ وكيف يمكن تحقيق المصلحة الوطنية؟.

وتعد دراسة المقايضة للنظام، أساساً رئيساً لعملية هندسة النظام وتصميمه. ومن الأهمية بمكان، إدراج الاعتمادية ضمن مبادئ عناصر المقايضة، من حيث التكلفة والأداء عند اعتبار أي تغيير هندسي في التصاميم، وليس عيباً إشراك جميع المهتمين بصناعة الشبكات، من صنَّاع، ومطورين، ومقدمين للخدمة، ومناقشة التصاميم للخروج بنظام هندسي، ومخطط صلب، لشبكة مفتوحة لا تملكها جهة منفردة، تكون مسؤولة عن تهيئتها وتطويرها والمحافظة على أمنها. فالهدف الأساس، الخروج بتصاميم متينة وتكوينات قوية لمقاييس تقنية، وممارسات تجعل القرارات الضرورية المطبقة على جزء فرعي من الشبكة أقرب للمثالية في كامل النظام. كما أن التنسيق بين الهيئات، والمنظمات الصناعية، وتطبيق المعايير القياسية العالمية، والمحلية، والحوار التقني، أساسية لجمع المصممين وصنَّاع المعدات والأجهزة ومقدمي الخدمات، وشركات التجميع والتركيب، وهو أمر في غاية الأهمية، لضمان تقديم نظام يتمتع باعتمادية وموثوقية عالية.

اعتبارات البيئة الأمنية للشبكة:

تتأثر الاعتمادية كثيراً ببيئة الشبكة الأمنية، الموجودة ضمن تصميمها الأساسي، لذا؛ فإنه من الضروري تفهم الأولويات والمزايا القابلة للمقايضة، مقابل الأمن، وبخاصة مزايا التهيئة الافتراضية «Default». وكثيراً ما توجد ثغرات أو طرق للاختراق مكتشفة ومعروفة في بعض الأنظمة، وتسعى الشركات المالكة لتلك الأنظمة لتوفير أدوات وإجراءات قياسية لتلافيها. ومن العوامل المهمة لتحقيق الاعتمادية، المحافظة على أمن ملف حفظ كلمات المرور، وصلاحيات مستويات الدخول، لرؤساء ومدراء التشغيل، وسلامة سجلات الدخول للنظام، وقدرات المختصين لاكتشاف الاختراقات. ولأنه لا يمكن أن يعامل أمن النظام بمعزل عن تحليلات بيئة التهديدات؛ فإنه يجب فهم وتحديد الأدوات والتقنيات المتوفرة للمهاجمين، إذا ما كان هناك إصرار على مقاومة الاختراقات وتلافيها. ولهذه الأسباب، فإن الالتزام الدقيق بإجراءات الأمن في جميع عناصرها أمر ضروري، يوجب تقييمها في كل مرحلة من مراحل إجراءات التشغيل، بما في ذلك إجراءات التحكم الإداري لمعرفة مدى وسرعة الاستجابة لتعطل الشبكة. وهناك عدد آخر من وسائل التحكم الإدارية وتشمل، على سبيل المثال: إجراءات إعادة تهيئة الشبكة، وزيادة الإجراءات الأمنية، كردة فعل لمحاولات الاختراق، أو تخفيض الوظائف التشغيلية للحد من الصلاحيات. إن مثل هذه الإجراءات تساعد كثيراً على احتواء الأعطال، وتمنع انتشارها وتقلل من آثارها السلبية. كما أن هناك حاجة لاختيار أفضل الوسائل من بين الإجراءات، للاستجابة الفعالة أثناء الحدث الفعلي. وعند تطبيق هذه الإجراءات والقواعد، ودعمها بالتجارب التشغيلية المكتسبة؛ فإنه يمكن أن يؤدي ذلك إلى توفير اعتمادية عالية للشبكة، وتكوين قاعدة بيانات تكون أساساً لعملية هندسية ملموسة. ومن الضروري حماية هذه الإجراءات ونتائج التحليل بعناية فائقة لمنع أي شخص غير مصرح له من الوصول إليها، حتى لا يسيء استخدامها في معرفة نقاط ضعف النظام.

ولأن الناس على وجه العموم يرحبون بكل ما هو مشروع ويتقبلونه بحماس كبير؛ لذا فإن تطبيق وسائل مبنية على مستويات محددة وواضحة ومصدقة من قبل هيئة معتمدة، لفحص اعتمادية العناصر والمعدات والشبكات، يمكِّن الشركات من عمل مقايضات مبنية على معلومات موثوقة، ويساعد على تبني ثقافة الاعتمادية لدى المجتمعات التقنية. كما أن وضع لائحة للقوانين العلمية والمعايير المجمع عليها المتعلقة بالتصاميم والإنشاءات واتباع التعليمات، مثل أنظمة

الإنشاءات الكهربائية، والأنظمة الإنشائية، يقلل من خطر تعطل شبكة الكهرباء، أو سقوط المباني، ويوفر فحوصات مقننة ودقيقة للاعتمادية، وسيكون للشهادات المصدقة للمنتجات قيمة عالية، كوحدة قياس لمقارنة المنتجات، والمعدات المستخدمة في البنية التحتية.

ولا يخفى على أي دارس أن توفير بنية تحتية مأمونة، يعد في غاية التعقيد، لأنه من الضروري أن تتمشى استراتيجية أمن البنية التحتية مع احتياجات العمل، ومع مستوى المخاطر المقبولة. ولابد أن تتعامل الأنظمة الوقائية مع نطاق واسع من التهديدات، بما في ذلك الفيروسات، والرموز العدائية، والمخترقين، والكوارث الطبيعية المتوقعة، والتخريب الإرهابي المتوقع. ومن الضروري ـ أيضاً ـ تجهيز واستخدام أدوات أمنية متنوعة، بتكاليف متعادلة مع تأثيراتها، بما في ذلك أدوات مراقبة المحتوى، وكشف الاختراقات، وأدوات قادرة على كشف أي حدث يحصل في جميع نقاط التواصل والربط مع الشبكات ونقاط التحقق من صحة البيانات، ووسائل تشفير البيانات والرسائل، والتحقق من الشخصية. وتهدف جميع الأدوات والوسائل السابقة لمواجهة التهديدات والتحديات المتوقعة، وضمان إيجاد بيئة عمليات آمنة، تعمل في الوقت نفسه بكفاءة عالية. ومن المهم الاستمرار في تطوير دفاعات لمواجهة الاختراقات، الداخلية والخارجية، مع عدم المبالغة، ومراعاة التحكم المتقن في إدارة وتكاليف البنية التحتية. والتركيز على التطوير والجاهزية، والفاعلية للشبكة.

وهناك أمر آخر؛ يعد في غاية الأهمية وهو الاستمرار في مواصلة تطوير عرض نطاق النظام، ليتماشى مع السرعات والأحمال المتزايدة، وتجهيز البنية التحتية للحلول الأمنية الآمنة للجيل القادم من الأنظمة، و هذا يؤدي إلى تلافي الاختناقات، والعمل المستمر على تقليص وخفض أعطال الخدمة، وزيادة الفاعلية إلى أقصى حد ممكن. وهناك متطلبات أساسية: منها ضرورة وضع استراتيجية ومعمارية قادرة على توفير قواعد مبنية على احتياجات العمل، لضمان أمن البنية التحتية، لجميع المؤسسات و المنظمات. وتوفير توازن بين أداء النظام وكفاءة الأمن والسلامة، ويمكن تحقيق ذلك بوضع بنية تحتية لإدارة العمل.

ومن الضروري بمكان وضع حلول لأمن النقاط الطرفية لشبكات الاتصالات، ونقل المعلومات، بهدف توفير حماية شاملة، وذلك باستخدام برامج حماية من الفيروسات، وبرامج جدران نارية، وبرامج تحكم في البرامج التطبيقية، مما سينتج عنه مواجهة للتهديدات المتنامية

الموجهة لبيئة الشبكات المتباعدة. ومن الضروري التوسع في إنتاج أدوات المستخدم النهائي end user tools، واستمرار الحرص على سرية وصحة توافر البيانات. ويتطلب ذلك إنشاء بنية تحتية لتطوير تقنية الشبكات، لضمان تحقيق جميع الإجراءات الأمنية باعتمادية وموثوقية عالية.

ومن المؤكد أن جميع الشبكات لا تخلو من معلومات مهمة وحساسة، لذا؛ من المهم التركيز على وضع حلول أمنية تقنية، بهدف حماية تلك المعلومات والبيانات من إطلاع غير المصرح لهم عليها، بما فيهم المستخدمين العاملين في المؤسسة، ووضع حلول لضمان صحتها، مع الحرص على سهولة تسجيل المعلومات وتأكيد اعتماديتها. ولأنه ما لم تتوافر المعلومات، والخدمات، فور طلبها؛ فإن البنية التحتية تصبح غير فاعلة؛ فإنه لذلك من الضروري وضع حلول لضمان توافرها، وإتاحة ما يحتاجه المستخدم من المعلومات، ودعم المرونة، واستمرار الحالة التشغيلية، وسرعة الوصول بموثوقية. ولتحقيق ذلك؛ فإنه يجب تطوير أدوات لإدارة المخاطر، وأدوات للإبلاغ الفوري، تشتمل على مجسات، وإشعارات للأداء، وسلامة أدوات القياس، وإجمالي البيانات، والإبلاغ عن أي تراجع في نظام الإبلاغ في البنية التحتية والعمليات.

(٢) المحور التشغيلي:

تخضع الاعتمادية لمدى تأثير عنصر، أو مكون محدد، من مكونات الشبكة على الأداء العام لذلك النظام، ويمكن القول أن الأنظمة القوية، تكون قوية عندما يسمح التشغيل العام للنظام، بحصول أعطال في بعض أنظمته الجزئية، دون توقف العملية التشغيلية، وهو الهدف الذي يسعى المختصون لتحقيقه. ولإمكانية تصنيف هذا النوع من الشبكات، وتحديد مكامن قوته وضعفه؛ فإنه يلزم أولاً: تحديد سياسة التشغيل للنظام ومفهومه، مع توفير شرح وافٍ ومفصل عن استخدامات شبكة المعلومات، بما في ذلك قوائم التشغيل المتعلقة بقدرات الدخول من خارج النظام، وإمكانية تنفيذ الأوامر عن بعد. كما أنه من الضروري معرفة طبيعة ومستوى التحكم في الحاسوب. وكيفية استجابة النظام للأعطال، والإعاقة، وتغيير البيانات. وكذلك المعرفة الدقيقة بهيكلية الشبكة، ونظام تدفق المعلومات منها وإليها. ولا يتحقق ذلك إلا بإيجاد وصف فني مفصل، ودقيق للشبكة، عن طريق توفير التصاميم والخرائط الإنشائية والرقمية، (Physical & Logical)، وتجهيزها لمدراء التشغيل والصيانة، مع سهولة الوصول إليها، ومن المهم أن تشمل تلك الخرائط توضيح دقيق لانسياب المعلومات وتدفقها، وتحديد

واضح للنهايات الطرفية الأساسية، ونقاط الاتصال والربط، والاهتمام بكيفية تعامل كل جزء من الأجزاء الفرعية للنظام، مع بعضها بعضاً في الظروف العادية وغير العادية، ومدى تقبلها للأعطال والأخطاء، والتأخير، والتقصير، في نظام جزئي آخر. وهذه التحليلات توفر معرفة توضح نسبة الترابط والتشابك بين الأنظمة الجزئية للشبكة، وتوفر أدوات مفيدة، لشرح وتحليل، تدفق المعلومات، ومعرفة تامة بمعمارية الشبكة، وتسهم الأدوات والوسائل الرياضية الأساسية، والنماذج الحاسوبية، والتشبيه الحاسوبي، وتحليل التعاملات، في رفع مستوى الاعتمادية. ويجب تحديد القيود التشغيلية، وأعطال التصاميم المحتملة، وخاصة في مراكز التحكم، ومراكز تحديد عناصر استرجاع البيانات، والموانئ Ports والجدران النارية، أو أي نهاية طرفية مهمة، وخاصة العناصر، التي تتحكم فيها برامج لينة، وتحديد إذا ما كانت تحتوي على نقاط ضعف تؤدي إلى تقويض الاعتمادية العامة للشبكة.

ومن الإجراءات، التي كثيراً ما تهمل، وضع سجل لحصر الحوادث التي طرأت على الأنظمة الحساسة، أو الرئيسة، والمعدات والأدوات، وتسجيلها، بهدف تحليلها والعمل على تلافيها مستقبلاً، والحرص على استخدام نظام كشف الشخصية، ونظام الإنذار، لتوفير مراقبة فعالة، ووسيلة إبلاغ آلية فورية لأدوات النظام الحساسة، والمهمة، والبرامج التطبيقية، وموانئ الدخول للنظام. ومن أهم عناصر البنية التحتية المحتوى وبيانات قواعد المعلومات؛ لذلك فإنه من الضروري تضمين الاستراتيجية التشغيلية، قدرات كافية لمراقبة المحتوى، بهدف حمايته من هجوم الرموز Codes والأوامر العدائية Malicious Commands، التي لا تستطيع برامج الحماية من الفيروسات اكتشافها، وذلك باستخدام نظام لمراقبة صحة البيانات الحساسة وسلامتها والتأكد من عدم تغييرها.

وأخيراً؛ فإنه يجب توفير خارطة طريق تقنية، وإجرائية، وتنظيمية، لتحقيق بنية تحتية آمنة، ولا يمكن تحقيق ذلك إلا باتخاذ وسائل وقائية وتجهيز حلول أمنية من أهمها: إيجاد تعليمات واضحة لتهيئة الأنظمة، وممارسة إدارية محكمة للنظام والشبكات، تشتمل على السياسات، والمقاييس، المعيارية وطريقة العمل، والأداء، والأدوار التي تؤديها المؤسسة أو المنظمة. ومن الضروري ـ أيضاً ـ وضع حلول مناسبة لطريقة الدخول للنظام، والمراقبة، والإبلاغ، تشتمل على كشف الاختراقات، والحماية من الفيروسات، ومراقبة المحتوى، وتسجيل الحوادث، وتسجيل الاستجابة للحوادث، والأمور الجدلية. كما ينبغي إنشاء أو تحديد هيكلية منطقة آمنة Security

Zone، موثوقة في شبكة الخدمات اللاسلكية، والإنترنت، وشبكة النطاق المحلي «LAN»، والنطاق الشبكي العريض «WAN»، والشبكات الخاصة، وشبكات الاتصالات الهاتفية. ومن المهم كذلك، وضع حلول لإدارة الثغرات الأمنية، وتشتمل على القضايا الإجرائية، والتقنية، لتقييم واكتشاف وتحديد الأولويات، والحد من ثغرات تطبيقات النظام، بأسلوب شمولي، وفي زمن استجابة سريع. وكذلك وضع حلول تشفيرية للتخزين، والتراسل، مثل أدوات تشفير للمستخدم النهائي، ووسائل تخزين احتياطية مشفرة، ومخازن الكترونية آمنة. وحلول للإبلاغ الأمني، تقوم على ضم عمليات المعلومات مع إجراءات إدارة الأمن والسلامة.

(٣) المحور البشري:

إن العنصر البشري يظل حاضراً في جميع شبكات البنية التحتية، كمدراء نظام، ومشغلين، ومهندسين، وفنيين، وعملاء، ومستخدمين. لهذا؛ فإن العامل البشري يضع السيطرة البشرية في دائرة التحكم العامة للنظام، من خلال مفاتيح التحكم، والشاشات، والمجسات الإلكترونية Sensors، ومخططات المعدات. ولا شك أن هذا يجعل إهمال وتساهل المشغلين وعدم يقظتهم، وارتكابهم أخطاء إجرائية، من أهم مسببات المخاطر الحقيقية. وقد جرت العادة في ظروف كثيرة أن يتلافى المشغلون، والمهندسون، الإجراءات التشغيلية وتهيئة النظام المعتمدة بحسن نية، مما ينتج عنه إضعاف اعتمادية النظام. لذا؛ فإن الاعتمادية الشخصية للأشخاص المهمين في دائرة التشغيل تعد من أهم الأمور الحساسة، الواجب التأكد من سلامتها لدعم اعتمادية النظام، مما يجعل الفهم الشامل لتأثير بيئة العنصر البشري أمر مهم للتقييم الشامل لنقاط الضعف في الشبكة. كما يتوجب التزام الحذر، واتباع ثقافة التعليم المستمر، لكل العاملين، من مشغلين، ومدراء، ومهندسين، وفنيين، لتطوير الاعتمادية. ومع أنه من السهل أن يتفق الجميع على ذلك؛ إلا أنه غالباً ما يتم تجاهلها عملياً.

وفي نهاية المطاف؛ فإن الاعتمادية تعد مبادرة، ومشروعاً بشرياً، وفي معظم الحالات العملية، يكون التعامل بين الآلة والإنسان جزءاً لا يتجزأ من النظام. لذا لابد من التأكيد، والتشديد على الإجراءات الكفيلة بضمان استمرارية يقظة العناصر البشرية، وتمكنهم، ووعيهم التام المستمر، لحالة النظام. وكذلك الوصول لمستوى عالٍ لموثوقيتهم واعتماديتهم الشخصية، علماً أنه لا يوجد حل سهل لتحديات الاعتمادية، كما أنه لا يوجد حلول دائمة لها.

إلا أن تطبيق جميع هذه الإجراءات والقواعد مع التجارب التشغيلية المكتسبة، بالتزام دائم، يحقق اعتمادية عالية للشبكة، وتكوين قاعدة بيانات تكون أساساً لعملية هندسية مأمونة، وتعطي تأكيدات مقبولة تتناسب مع الأهمية، التي يضعها المجتمع على البنية التحتية التي يمكن الاعتماد عليها.

اعتبارات فنية لمساندة العنصر البشري:

لتمكين العنصر البشري من أداء مهماته بكفاءة عالية؛ فإن ذلك يستلزم الاهتمام بأدوات وآليات محددة، تشمل الإنذار المبكر للأنشطة الغريبة، سواءً التي تأتي من النظام نفسه، أو من خارجه، فالإنذار المبكر لنشاط متوقع، أو نشاط فعلي، في البنية التحتية العامة، يمكِّن الجهات المعنية، من اتخاذ إجراءات لتلافي، أو تقليص إمكانية توقف الشبكة. كما أن الوسائل التشريعية العادلة، في حدود تنظيمات واضحة لتدفق سريع وآني للمعلومات الاستخبراتية، والحوادث، بين الحكومات والمنشآت والمصالح العامة، وخاصة تلك التي تصب في حماية البيانات الحساسة للأعمال والموارد والطرق، سيكون لها تأثير كبير لتوضيح بيئة التهديدات، ويحقق استجابة فعالة للحماية، ويمكِّن من تسليط الضوء على بعض التهديدات؛ وعلى الأخص المتعلقة بشبكة الإنترنت العامة، وهذه التهديدات يتم تحديدها عند تدفق البيانات من قبل عدد من مكونات وعناصر النظام. وهناك عدد كبير من الأمور غير الطبيعية الصغيرة منتشرة على مستوى كبير وغير ملحوظة، كأمور منعزلة، ولكنها عندما تتراكم وتترابط فإنها تصبح مؤشرات لمشاكل منهجية.

اعتبارات الإبلاغ وتمرير المعلومات:

من أهم متطلبات الاعتمادية، إنشاء نظام استجابة سريع، لاحتواء ومقاومة وإبلاغ الجهات المعنية، عن أي حدث يؤثر سلباً على كفاءة البنية التحتية، ومستوى الإنتاجية وكفاءة المؤسسات، والشركات، التي تقدم خدمات البنية التحتية. ومن المهم جداً تطوير هذا النظام ورفع كفاءته وتطبيقه، واتباعه، بدقة، ووضع إجراءات تبليغ دقيقة. فالمراقبة الذاتية، والمعالجة الذاتية لشبكات المعلومات، ليست صعبة المنال، إلا أن المسؤولية لتحديد المشكلة واتخاذ الإجراءات لتلافيها، تقع بكاملها على العنصر البشري. ويمكن الاستفادة من بعض التطابق في تقارير الإبلاغ عن مستوى الاعتمادية المنتشر في الصناعة مثل: نظم الإبلاغ في

أنظمة المحاسبة المالية، التي أنشأها مجلس المقاييس للمحاسبة المالية Financial Accounting Standards Board. كما ينبغي أن تستفيد شركات القطاع الخاص، التي تقدم خدمات البنية التحتية من بعضها بعضاً، في كل ما يتعلق بالاعتمادية. وهناك حاجة ماسة وعاجلة ـ أيضاً ـ لوضع آلية لتبادل المعلومات في حوادث الثغرات الأمنية، والحلول التقنية، وأفضل الممارسات التي يطبقها مدراء الأنظمة. مع مراعاة سرية الملكية والمعلومات الحساسة للشركة، في حدود الأنظمة. ويعد تبادل المعلومات الأمنية في قطاع شبكات الاتصالات، من أبرز الأمثلة التي نشاهدها كنتائج للمؤتمرات، التي تقام بين الشركات المعنية لتبادل البيانات فيما بينها وفي الحدود المسموح بها، ومثل هذه المؤتمرات ضرورية بين القطاعات، وخاصة عندما تطبق تقنية شبكات مشتركة. ومن الضروري كذلك أن تقوم مراكز التحكم في شبكات البنية التحتية بدور نشر وتوزيع معلومات بصورة منتظمة، على غرار ما تقوم به التلفزيونات العالمية من نشر للأخبار وتحذير من الكوارث، حيث أصبحت الفضائيات التلفزيونية مصدراً مهماً من مصادر توزيع المعلومات والإنذارات، التي تفيد المجتمعات عن طريق نقل المناظر والملاحظات الحية للحوادث. وما ينقص مراكز التحكم للقيام بدور مشابه هو الوسائل التقنية، والتشريعية، لتأليف بيانات من مصادر متعددة، وتشكيل استنتاجات فورية وهادفة، وهذا مجال يمكن أن تعمل فيه الحكومات والصناعة مجتمعة لتحقيق المصلحة العامة.

تصميم مخططات بيانية لتوضيح أنواع ونماذج الفشل:

من الضروري إيجاد مخطط بياني لنماذج الفشل لأي نظام أو شبكة يوضح كيف؟ ولماذا؟ تحدث أعطال شاملة في الشبكة. وهذه المخططات تعد تصورية وليست كمية، لكنها مفيدة لمقارنة أحداث حقيقية، مع بدائل افتراضية، كما أنها تؤكد وتعالج بدائل لإظهار ثغرات محتملة، وتحلل المخاطر والمكاسب لاستراتيجيات التعامل مع العجز والقصور، لأن التجارب التاريخية (الماضية) تتركز في الغالب، في جزء واحد من النظام، وأن معظم تحديات اعتمادية الشبكات لم تجرب بعد. كما أنها توضح نقطة أساسية، وهي حالة اعتمادية كامل الشبكة، عندما تهددها تحديات الاعتمادية. فالواقع أن المخططات البيانية لاحتمالات الفشل المتعلقة بأعطال الشبكة تفسِّر جميع الأحداث ذات التأثير المتساوي في الضرر، والمميِّز المهم في جميع الاحتمالات، هو مستوى إمكانية حدوثها. وفي الغالب فإن هناك احتمالين يجب أخذهما في الحسبان: احتمال أن الحدث سيحل، واحتمال أنه لو حدث العطل فسينتج عنه فشل شامل،

وهذا يجعل الاحتمال النهائي «محصلة نتاج الاحتمالين» مؤشراً لمدى خطورة التهديدات. وعلى سبيل المثال: يمكن اكتشاف أن فشل قطعة أو جزء إلكتروني سيتسبب بكل تأكيد في إنتاج سلسلة من ردود الفعل، التي تسبب عطلاً شاملاً للشبكة، وأن فقدان محول مستقل أو مقسم أو مجس لن يتسبب في فشل شامل للنظام. وعلى المنوال نفسه يعد سقوط نيزك أو جرم سماوي على جزء من الشبكة في غاية الندرة، إلا أن حدوثه ممكن، ولكن إذا حدث ذلك، فإن احتمال حدوث تدمير وتوقيف للبنية التحتية للشبكة يكون كبيراً. إن مثل هذا التحليل يساعد كثيراً على فهم الأولويات النسبية لتهديدات الاعتمادية. وهناك المزيد من الأسئلة، التي تحتاج إلى إجابات عن تصنيف تهديدات الشبكات العالمية، واختراقات القراصنة حقيقة غير مقبولة، ولكن احتمال أن يبدأ القراصنة في إحداث سلسلة لردود فعل تتسبب في حدوث أعطال مؤثرة في الشبكة يبقى وارداً، ورغم أنه لا يحظى بالاهتمام اللازم، لكنه يحتاج إلى تحليل مفصل بعناية. كما أن احتمال حدوث هجوم منسق على شبكة الإنترنت، واحتمال أن يكون مؤثراً عند حدوثه، يحتاج هو الآخر إلى تفحص وتدقيق.

ومن الضروري إجراء تحليل دقيق لحالات محددة، توضح الثغرات ونقاط الضعف المحتملة، وتساعد على تحديد القراصنة الناشطين، الذين يحظون بقسط وافر من النجاح، وتحقق التحاليل نتائج ناجحة في شبكة معقدة، وتبين ردود الفعل الناجعة لتتبع الهجوم المنفَّذ، و فهم طريقة الهجوم، وإمكانية حدوثه، ونوع الأعطال المتوقعة.

(٤) محور القرصنة الإلكترونية والإرهاب:

مهما كانت أهداف القراصنة؛ فإن خطرهم على شبكات البنية التحتية، لا يقل عن خطر الإرهاب الدولي. فالإرهاب الدولي يعمل على تفجير البنية التحتية مسبباً خسائر مادية وبشرية ومعنوية لخصومه، أما القراصنة، أو إرهابيو المعلومات، فإنهم يصلون النتيجة نفسها عن طريق تدمير قطاعات التقنية، ونقل المعلومات، إما كجزء من الإرهاب الدولي أو لأهداف أخرى. وقد يكون الاختلاف الوحيد بين الفئتين، هو الأهداف والنوايا. وبالإضافة إلى ما يتسبب فيه الإرهاب من خسائر في الأموال والأنفس، فالإرهاب قد تسبب في خسائر كبيرة، لمجرد الاستعداد لمواجهته وتلافي أخطاره، ففي مجال تحقيق الأمن المعلوماتي، ووفقاً لتقارير قسم الدراسات والأبحاث في مؤسسة «إيبوك eBook» ميسي فرانكفورت، تشير الدراسات إلى نمو

كبير في السوق العالمي لمنتجات وخدمات الأمن المعلوماتي بسبب الضغوط الأمنية والتطوير الدائم لحلول الأمن المتطورة، حيث تجاوزت قيمة السوق ٧٩ مليار دولار في عام ٢٠١٠م.

اعتبارات الحماية من القرصنة الإلكترونية

أنظمة حماية مزوِّد الشبكة العالمية Web Servers:

إن معظم عمليات تزوير البيانات وتغييرها ومنع الخدمة عن المشتركين والمستفيدين، تقع نتيجة للاختراقات الإلكترونية الناجحة، التي يحققها القراصنة، وإرهابيو شبكة الإنترنت. وكما سبق التنويه عنه؛ فإن السطو الإلكتروني على قواعد المعلومات في تزايد منتظم، مما يستوجب رفع مستوى اليقظة، والاهتمام لدى المؤسسات الحكومية، والتجارية، لحماية المعلومات والأصول الرقمية من العابثين والمهاجمين بجميع فئاتهم. والمؤكد أن مستوى اليقظة والاهتمام بأمن البيانات متباين بين الشركات، والمؤسسات العامة والحكومية، إذ لازال المهاجمون يحظون بفرص كثيرة لتزوير المعلومات وتغييرها، أو سرقتها. وكما سبق إيضاحه بالتفصيل؛ فإنه يصعب اكتشاف المخترقين في المستويات التشغيلية للشبكة، لأن بإمكانهم التخفي كمتعاملين شرعيين، أو لكونهم يدخلون ويخرجون دون ملاحظة بسبب ازدحام الشبكة؛ غير أنه من الممكن اكتشافهم في معظم الشبكات بتتبع آثارهم وليس بإدراك علامات تواقيعهم. كما أن استخدام الأدوات الجيدة المصممة للكشف المبكر عن أي عمل غير معتاد في الشبكات المستهدفة، وتقدير أضراره، يساعد مدراء الأنظمة المتمكنين من القيام بأعمال تصحيحية قبل تفاقم مشاكل مؤثرة. وحماية مزوِّد الشبكة ليس بالأمر السهل، لأنه بطبيعته يحتاج إلى أن يكون مفتوحاً على الشبكة العالمية، وأن يكون في الوقت نفسه مقيداً ومحمياً ضد المهاجمين، بالإضافة إلى أن مجارات التطور التقني الأمني ومتابعة التحديثات المستمرة، والتدقيق والتحقق اليدوي، يعد عمل يوم كامل، وهذا يصْعُب على معظم المؤسسات الحكومية، والشركات، إذ ليس لديها ما يكفي لذلك من الوقت والمصادر، أو حتى الخبرة الأمنية المتكاملة، لتحقيق أمن إلكتروني قوي لشبكاتها وقواعد معلوماتها، مما ينتج عنه وجود ثغرات أمنية مؤثرة بين الممارسة الأمنية الصحيحة، والتطبيقات العملية للإجراءات والتعليمات الأمنية. ويمكن القول، إن أي مؤسسة أو شركة تمارس تقديم خدمات عامة، أو عمل تجاري، من خلال الإنترنت، لابد لها من وضع استراتيجية أمنية لمواجهة ثغرات الوعي الأمني، ويجب أن تكون الاستراتيجية متكاملة وشاملة لوسائل وأدوات الحماية من التهديدات المعروفة، وكشف التغييرات غير

الشرعية والقدرة على المعالجة الفورية للأضرار الناتجة من أي هجوم. بالإضافة إلى ذلك، فإنه يلزم الاحتفاظ بأي بيانات ضرورية، لتحديد نوع وهوية الهجوم، باستخدام آخر ما توصلت إليه التقنية الحديثة، من برامج الوسائط الأمنية، لحماية مزوِّد الشبكة، وتقييم مستوى الأمن بهدف تحقيق الحماية الأمنية التامة، مهما تعددت أجهزة المزوِّد وموانئ الوصول.

ومن متطلبات السلامة ـ أيضاً ـ أن تعمل الأدوات الأمنية الخاصة بمزوِّد الشبكة، على معالجة ثغرة الوعي الأمني، وتكريس الممارسة الصحيحة، لأمن المزوِّد الشبكي، وذلك بتقييم الأمن الإلكتروني وإدارته في عدد كبير من حاسبات خدمة الشبكة المتصلة ببعضها، حتى وإن كانت تعمل في بيئة مختلفة. إن هذه الأدوات تعمل من خلال المزوِّد المضيف، لتحقيق التدقيق الأمني وكشف أي محاولة وصول غير مشروعة، فهي تقدم عمق أمني وغطاء أمني لا يمكن أن يقدمه أي ماسح شبكي عادي. ومن الضروري كذلك؛ استخدام وسائط وبرمجيات حماية قادرة على تهيئة قوية وشاملة لمنع السطو على المعلومات، باستخدام آخر ما توصلت إلية التقنية. ويتطلب ذلك إجراء تقديرات لمستوى الأمن والسرية المتوفرة في أنظمة مزوِّد الشبكات العالمية، مهما تعددت نقاط وموانئ الدخول للشبكة ومصادر التهديدات. بالإضافة إلى تحديد الثغرات الأمنية، التي تحدث أحياناً عند تهيئة بيئة النظام، وتحديد إمكانيات وقدرات برامج التشغيل، ومنع المخاطر الناتجة عن فتح موانئ غير مقصودة، يمكن أن يتسلل عن طريقها العابثون وسارقو المعلومات بإغلاق تلك الموانئ، ووضع نظام مراقبة مستمرة يكشف محاولات التسلل ومنعها أثناء حدوثها. وفي حالة نجاح أي محاولة للاختراق، فإن على نظام الحماية، إما بصورة تلقائية أو يدوية (حسب تهيئته الأساسية ورغبة مدير أمن الشبكة المسؤول) أن يقوم بتصحيح الملفات المتأثرة، وإعادته لحالته السابقة، وبذلك يعود الموقع لحالته الطبيعية بسرعة مقبولة.

ومن الضروري أيضاً تشغيل حوائط نارية ذات كفاءة عالية في جميع الحواسيب ومزوِّدات الخدمة Servers التي تتحكم في الشبكات، والابتعاد عن البرامج غير مضمونة المصادر، وعزلها تماماً عن حواسيب الشبكة، حتى لا تتسبب في الإضرار بها. كما أنه من الضروري؛ استخدام برامج مضادات الفيروسات، بعد أن أصبح بالإمكان نشر فيروس في جميع أنحاء العالم في مدة خمس دقائق، أو نحو ذلك، من خلال عدة طرق، منها البريد الإلكتروني، الذي بمجرد وصوله إلى الضحية وفتح الملف المرفق للرسالة، والحامل للفيروس، فإن الفيروس يحمِّل نفسه في جميع العناوين المدرجة في البريد الإلكتروني. ومن الإجراءات الواجب الحرص عليها؛ إضافة

تحديثات برامج التشغيل، سواءً كانت بيئة التشغيل ـ ويندوز ـ أو ـ ليونيكس ـ أو أي بيئة أخرى، فمعظم المشكلات الأمنية، التي يتعرض لها مستخدمو الحواسيب، تكون بسبب وجود ثغرات في منتجات الشركات (بما فيها مايكروسوفت)، وبخاصة البرامج التشغيلية والتطبيقية. فالفيروسات وبرامج التجسس التي تهاجم الحواسيب، تحمِّل نفسها علي تلك الأجهزة، بسبب الثغرات في برامج التشغيل. ويجب استخدام برامج الحماية من التجسس، واختيار الأفضل منها، لأن القراصنة الذين يهاجمون الشبكات الإلكترونية يحرصون على مراجعة المعلومات التي تصل إليهم عن طريق برامج التجسس، التي يرسلونها لأهدافهم وتطويرها، في محاولة لاستخلاص المعلومات الخاصة، التي تمكنهم من سرقة البيانات والمعلومات السرية. ولتحقيق مستوى مقبول من الأمن الإلكتروني؛ فإنه يجب أن تتضمن الحماية وسيلة للتدقيق الأمني الإلكتروني في جميع العناصر البيئية، المتعلقة بأنظمة مزوِّد الشبكة، بما في ذلك التحقق من النسخ المستخدمة، من حيث أصلها، ومصدرها، والشركة المصنعة، وتجهيزات النظام، والإصلاحات الفورية (HOT FIXES)، وتجهيزات كلمات المرور، وقوائم التحكم في الدخول، وبقية عناصر أمن النظام، وبرمجيات التشفير. ويجب استخدام أنظمة أمن معلومات قادرة على تحديد المخاطر الأمنية، وتقديم وصف للمشكلة وتعريفها بدقة، واقتراح الحلول المناسبة لكل مشكلة.

ومن المشاكل المتكررة في مجال شبكات نقل المعلومات الواجب تدقيقها بانتظام، ما يلي:

- تعرض مزوِّد الشبكة لتغيير غير مشروع في عناصر تهيئته الافتراضية وتجهيزاته (Configuration Settings).
- تغيير صلاحيات فتح الملفات.
- تغيير صلاحيات الدخول لحسابات المشتركين الرسميين.

ويعتمد التدقيق الأمني كثيراً على تعليمات المصنعين للمعدات، ومنتجي البرامج الأصلية، وما يصدر عنهم من ملحوظات، وتعليمات، ونصائح أمنية لمنتجاتهم. ونظراً للتطور التقني السريع؛ فإنه من المهم توظيف باحثين متخصصين، لمتابعة التطور التقني في مجال أمن المعلومات، وتتبع تقنيات قراصنة المعلومات على المستوى العالمي. وهناك ثلاثة مبادئ تعد في غاية الأهمية للحفاظ على أمن مقبول لمزوِّد الشبكة، وهي «أمِّن ـ اكتشف ـ بلِّغ»، وفيما يلي شرح لهذه المبادئ الثلاثة:

١ . مبدأ الأمن الإلكتروني لمزوِّد الشبكة:

بعد تقييم النظام وحل جميع القضايا الأمنية المتعلقة به، يتم قفل جميع الموانئ غير المستخدمة، وخاصة موانئ المزوِّد «متعددة الوصول»، وهي البوابات التي تسمح لعدد كبير من الأدوات Devices بالمرور من خلالها، مما يساعد على منع أي محاولة دخول غير مرخصة، وضمان استعادة سريعة للنظام فيما لو جرت مهاجمته. وكذلك يتم قفل وتأمين بيئة المزوِّد، بحيث يستحيل تغيير المحتوى، وعمل نسخة كاملة لملفات تجهيزات المزوِّد الشبكي، وملفات المحتوى، وتخزن النسخة الاحتياطية في حاسب آخر إن وجد، أو في نفس وسائل تخزين المزوِّد الشبكي، وكذلك المحافظة على حالة القفل التام لمداخل النظام غير المعتمدة، بعد ذلك يتم مراقبة النظام بواسطة برامج متطورة، تعطي إنذارات وتمنع دخول أي تسلل للنظام.

٢. مبدأ اكتشاف التغيير أو محاولة التغيير:

ويعني ضرورة استخدام أنظمة مراقبة متطورة، باستخدام آخر ما توصلت إليه تقنية أمن المعلومات، لضمان اكتشاف أي تغيير، أو محاولة تغيير، لموانئ الوصول المقفلة، أو أي محاولة للوصول، لقواعد المعلومات أو المحتوى، وإرسال إنذارات دقيقة، لمسؤول الأمن في المؤسسة. عند حدوث أي محاولة سطو على أي جزء من النظام. ويمكن أن تصمم عملية المراقبة الإلكترونية للنظام، بحيث تشمل عدة خوادم، موزعة لدى مضيفين متعددين، وتكون المراقبة متزامنة في جميع أجزاء الشبكة، كما يمكن أن يصمم النظام، لتصحيح الخلل الحادث من عمليات السطو الإلكتروني بصورة تلقائية، أو يدوياً، وبذلك يمكن ضمان استمرارية عمل النظام وإعادة تشغيله بأقل جهد إداري. كما أن دلائل السطو يمكن حفظها، لأغراض التحقيق والدراسة لتحديد هوية المهاجمين للنظام، وتحديد أسلوب المحاولة وتقنيات السطو المستخدمة لوضع حلول إضافية مستقبلية.

٣. مبدأ الإبلاغ وتحرير التقارير:

يتكون مبدأ التقارير من أربعة أجزاء على النحو التالي:

- تقارير تهيئة النظام (Configuration Reports): يحلل هذا التقرير عناصر

التجهيزات الفنية لمزوِّد الشبكة، ويحدد العناصر، التي تسببت في إحداث الثغرات الأمنية للنظام، حيث يتم تحليل ملفات تهيئة النظام (Configuration Files) وملفات إعدادات التسجيل (Registry Setting) بعناية فائقة، وكذلك إجراء تحليل مكثف على نسخ البرامج المستخدمة.

- تقارير المرور (Access Reports): يتم تحليل مستويات صلاحيات المشتركين المسموح لهم الدخول على النظام، لكل جزء من الموقع، ومن ثم يتم تحديد كلمات السر الضعيفة ويبلغ عنها.

- تقارير ثغرات الدليل (CGI and Vulnerable Directories Reports): هناك أكثر من ٥٠٠ فحص يمكن إجراؤها في هذا التقرير، حيث يجب دراسة جميع الملفات، لمعرفة أي ملف يمكن أن يستخدمه المهاجم للحصول على وسيلة دخول غير نظامية للشبكة، وتحديد أي ملف يحتوي على ثغرات أمنية، وتحذير مسؤول الأمن بخصوصه.

- تقارير الثغرات الأمنية في النظام (System Vulnerabilities Reports): هناك أكثر من ٣٤٠٠ فحص يمكن إجراؤها لتقييم الموانئ Ports والخدمات النشطة في النظام، مثل الموانئ شائعة الاستخدام من قبل القراصنة لمهاجمة النظام، وبالأخص البرامج الشائعة التي يحتمل احتواؤها على حصان طروادة، وكذلك الخدمات ذات الثغرات الأمنية، مثل Telnet & FTP، التي تفتح موانئ في النظام يمكن أن تستخدم للهجوم غير المشروع. بالإضافة إلى ذلك ولتوفير الحد الأدنى من أمن المعلومات؛ فإنه يفترض اتباع الإجراءات التالية:

عدم فتح رسائل البريد الإلكتروني مجهولة المصدر، فقد يكمن فيها أحد أخطر أنواع الفيروسات. وكذلك تفريغ محتويات البريد الإلكتروني من الرسائل التجارية، التي لا تهم المستخدم والتي ترسلها بعض الشركات للدعاية، دون معرفة أو إذن مسبق من قبل صاحب البريد الإلكتروني، والحذر من العروض المجانية، التي لا تخلو من الفيروسات أو برامج التجسس، أو كليهما معاً، واختيار كلمة سر معقدة تتكون من حروف وأرقام ورموز، وحفظها في مكان آمن . ومن ذلك ـ أيضاً ـ الحرص على عدم الدخول إلى المواقع غير الآمنة، وبخاصة مواقع قراصنة الحواسيب. وضرورة تدريب المشغلين، واختيار الكفاءات الجيدة للعمل في مجال المعلوماتية.

اعتبارات حماية المنشآت والتحكم في الدخول

يمكن القول إن مواقع البنية التحتية المهمة، مثل آبار البترول ومحطات الكهرباء ذات الأحمال العالية ومحطات الطاقة النووية، تحظى بحماية مقبولة إلى حد كبير. وخير دليل على ذلك فشل المحاولة الإرهابية، التي شنتها القاعدة على إحدى من أهم وأكبر آبار البترول في



شكل (٧): التحكم في الدخول

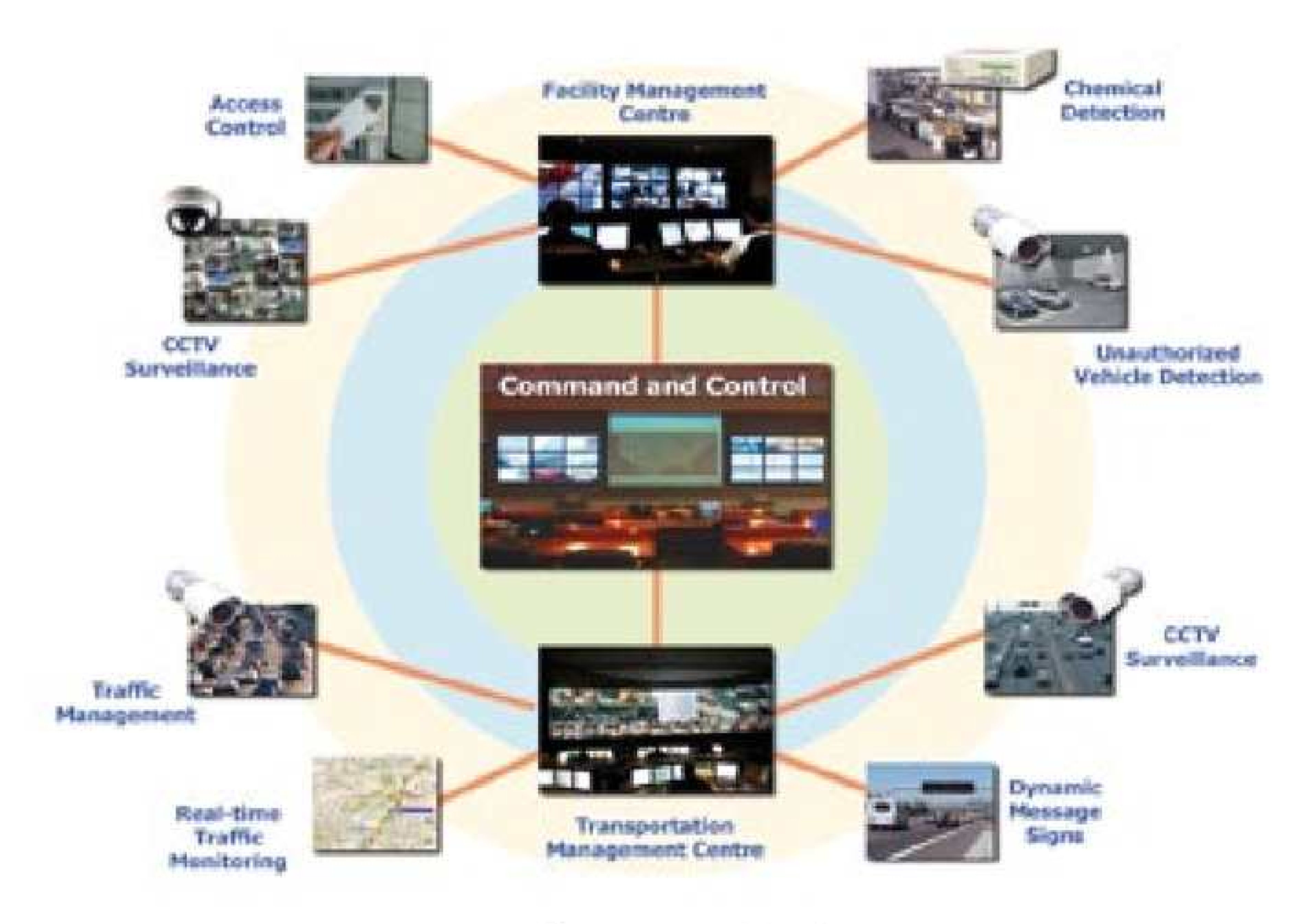
المملكة العربية السعودية، حيث لم يتجاوز المهاجمون الخط الدفاعي الثاني، كما ذكرنا سابقاً. لذا؛ فإنه من الضروري حماية المواقع الحساسة في البنية التحتية بعدد من خطوط الحماية التي يأتي في مقدمتها:

- استخدام الجدران العالية ويفضل أن تكون خرسانية.
- استخدام دوريات وحراسات مدربة مع استمرارية التدريب.
- إنشاء مرفق سيطرة وتحكم في النظام Command and Control، يحتوي على مركز إدارة أمن المرافق، ويضم معدات حيوية للتحكم في الدخول ومعدات كشف كيميائية Chemical Detection Equipments ومعدات كشف السيارات والمركبات غير المرخص لها بدخول الموقع، وكاميرات مراقبة عالية الجودة. ويتبع مركز السيطرة والتحكم مركز إدارة وسائل النقل والمواصلات، ويحتوي على إدارة الحركة باستخدام معدات إلكترونية وكاميرات مراقبة توضح حركة المواصلات حول المنشأة. ويمكن أن يضاف إلى ذلك إشارات رسائل متغيرة Dynamic Massage Signs، توضح للمرور حالة الموقع والاتجاهات المسموح المرور منها.

- استخدام البرمجيات المتقدمة والمتطورة للتحكم في الدخول، وتحديد وقت دخول وخروج الأشخاص المصرح لهم والزوار.
- إنشاء إدارة يقظة ومتمكنة لأمن المنشآت، وتزويدها بكل ما يستجد في تقنية الحماية الأمنية.

(٥) المحور الإعلامي

للإعلام دور مهم ومؤثر في مكافحة الإرهاب، فهو يوجه الرأي العام، ويصيغ مواقفه وسلوكياته، من خلال الأخبار والمعلومات، التي تزوده بها وسائل الإعلام المختلفة. والشخص، الذي لا يتوافر لدية القدر الكافي من المعلومات، والبيانات، لا يستطيع تكوين



شكل (٨): مرفق سيطرة وتحكم

موقف معين، أو تبني فكرة معينة، عن أي حدث يقع في محيطه وبيئته، مما يؤكد قدرة الإعلام، بكافة صوره وأشكاله، على إحداث تغييرات في مفاهيم وممارسات الفرد والمجتمع، عن طريق تعميم المعرفة، والتوعية، والتنوير وتكوين الرأي. فالإرهابيون والحكومات، ووسائل الإعلام يدركون دور ومسؤولية الإعلام، عند تغطيتها للحوادث الإرهابية، رغم تباين

وجهات النظر[٤٠]، فالرؤية المحركة لردود الفعل أثناء الحوادث الإرهابية؛ غالباً ما توفر مكاسب تكتيكية واستراتيجية للعمليات، وللوسائط الإعلامية. والمهم هو فهم ديناميكية المشروع الإرهابي، وتطوير سياسات لخدمة مصالح المجتمع والحكومات والإعلام. وبطبيعة الحال فقد أصبحت الوسائط الإعلامية جزءاً أساسياً من حياة الشعوب والمجتمعات، بفعل استجابتها ومواكبتها للتطورات والمستجدات، التي تحدث في شتى المجالات. وقدرتها على الوصول إلى الجماهير ومخاطبتهم والتأثير فيهم، لهذا؛ من الضروري أن تراعي وسائل الإعلام، ظروف كل مجتمع وبيئته الثقافية والفكرية، والعمل بفعالية في الاتجاه الصحيح، بما يدعم الأمن الوطني ومصالح المجتمع، بشكل يضمن احترام هوية ذلك المجتمع وخصوصيته.

اعتبارات تأثير الإعلام على الإرهاب

لقد بات من الضروري النظر في عدد من البدائل، التي يمكن اتخاذها لتحسين التعامل المثمر بين الحكومات والإعلام لمكافحة الإرهاب، عند ردود فعل كليهما للتغطية الإعلامية، وتشمل هذه الإجراءات تمويل مشاريع تدريبية مشتركة، وإنشاء مركز للمعلومات الإرهابية، وتنمية استخدامات المعلومات الصحفية، التي تتمركز حول حوادث الاختطاف وقوة تخليص الرهائن. وكذلك إنشاء مراكز للمعلومات، لدعم التطوع من قبل الصحفيين، لنشر معلومات موجهه تخدم الأمن الوطني، بالإضافة إلى مراقبة الإرهاب ضد الصحفيين.

ولأن العلاقات العامة المؤثرة، يجب أن تسبق الأحداث ولا تأتي كردة فعل بعد الحدث، لذا؛ فإنه يجب أن توظف الحكومات استراتيجيات وطنية واسعة لمجابهة المبادرات ذات التوجه الإرهابي، ويمكن أن يقوم الإعلام بدور فاعل في إطار هذه الاستراتيجيات. ومن الضروري ـ أيضاً ـ ممارسة تمارين تدريبية، تجمع المسؤولين في الحكومة مع المسؤولين عن الإعلام لإدارة حدث افتراضي، إذ إن هذه التمارين توضح لكل فريق وجهة نظر كل منهما، وتساعد في وضع استراتيجيات تحقق ما يصبو إليه الإعلام دون الإخلال بالعمليات الأمنية، الأمر الذي يتطلب إنشاء مركز حكومي دائم للمعلومات الإرهابية، التي تمكن الإعلام من نشر معلومات تخدم الأمن الوطني، بالاتفاق والتعاون مع المنظمات والهيئات الإعلامية، وربطها إلكترونياً مع المركز مما يحقق ردود فعل، وتغطية إعلامية سريعة ودقيقة عن الأحداث، وتنسيقها بحذر لجعلها تخدم المصلحة الوطنية، بحيث تحدد بوضوح موقف الحكومة من العملية الإرهابية.

ويمكن أن يترأس المركز مسؤول حكومي كناطق رسمي للمركز، أو ربطه بالهيئات الإعلامية، لطباعة الأخبار مباشرة في مكاتب الإعلام. كذلك يحدد هذا المركز الصحفيين، الذين يرشحون للحصول على معلومات من المنظمات الإرهابية، ووضع تلك المعلومات في المركز ليتم تحليلها ونشر ما يخدم الأمن الوطني منها، أو تأجيل النشر حتى ينتهي مفعولها السلبي على الأمن، ومنع الإرهابيين من تحقيق المكاسب الإعلامية أو الاستفادة منها. كما أن دعم استخدامات تجميع الأخبار والمعلومات الإعلامية يعد إجراءً مهماً أثناء تغطية أحداث اختطاف الرهائن، ويكون ذلك باستخدام مركز لتجميع المعلومات، التي يمكن نشرها أثناء معالجة الحدث، لخدمة عملية إنقاذ الرهائن، رغم أن تحقيق مثل هذا الهدف قد لا يكون سهلاً في ظل التقدم التقني وحرية التعبير والنشر. بالإضافة إلى ضرورة دعم تغطية إعلامية تطوعية موجهة، ويكون ذلك بإنشاء نظام سهل بحيث لا يحد من حرية الصحافة، لكنه يعمل على توجيه الإعلاميين لما يجب مراعاته أثناء تغطية الحوادث الإرهابية والتحقيقات الصحفية مع زعماء الإرهاب. ومن المفيد كذلك، عقد المؤتمرات الوطنية والإقليمية والعالمية لدراسة استراتيجيات النظام، الذي ينظم التقارير الإعلامية عن المنظمات الإرهابية والتعرف على مكوناته، لأن مثل هذه المؤتمرات سترفع من مستوى الفهم والإدراك لدى العامة، وتوضح ما يدور في المجتمعات السياسية، وتحدد السياسات الإعلامية، وتشرح مدى حاجة المؤسسات الرسمية لذلك. ويكون الهدف من هذه المؤتمرات الحد من نشر المعلومات المتعلقة بالرهائن، التي قد تضر بهم، مثل عددهم، وجنسياتهم، ومستوياتهم الوظيفية، ومستوياتهم المالية، وأهمية أقاربهم. وكذلك، الحد من المعلومات المتعلقة بتحركات رجال الأمن، والجيش، والحكومة، أثناء عملية الإنقاذ، وتقييد إذاعة المقابلات الشخصية الحية، غير المنقحة مع أعضاء المنظمات الإرهابية وزعمائها، وتفحص مصادر المعلومات، وبخاصة عندما توجد ضغوط عالية لنشر معلومات سريعة قد لا تكون صحيحة، والحد من التكهنات التي لا أصل لها، بالإضافة إلى تخفيض حدة المعلومات، التي قد تسبب إرباكاً للمواطنين، على نطاق واسع، وتساعد الإرهابيين على شحن عواطف المجتمع وزيادة الضغط على أصحاب القرار.

الخلاصة والاستنتاج والتوصيات

الخلاصة والاستنتاج والتوصيات

إن من أهم نتائج التقدم الهائل في التقنية الحديثة، وعلى رأسها تقنية وصناعة ونقل المعلومات، والانخفاض الكبير في التكلفة، والكفاءة العالية، والقيمة المضافة للأداء، هو تحفيز مكننة البنية التحتية، وتسهيل الوصول إليها، وذلك بربطها على المستوى المحلي والإقليمي والعالمي عن طريق شبكات الإنترنت العالمية، مما أثر على مستوى اعتماديتها وعرضها للخطر. وبما أن للاعتمادية آثاراً مباشرة بالمكاسب والأرباح، وكذلك الأمن الوطني والعالمي، فقد توجب على كل من القطاع الخاص والحكومي، الاستمرار في التجاوب مع التهديدات المتوقعة على الاعتمادية، بصورة منتظمة. والقلق اليوم هو: هل ستشعر الحكومات والمؤسسات الخاصة بخطورة الوضع وتقلل من نقص الاعتمادية وقصورها في بنيتها التحتية وبيئة التهديد المتغيرة باستمرار؟ أم أنه لابد للعالم أن يواجه كارثة شاملة في بنيته التحتية، لكي يتأهب ويضاعف جهوده لمحاربة الإرهاب؟.

لقد حان الوقت لتأسيس بنية تحتية ذات اعتمادية عالية تقوم على بيانات حقيقية وحقائق صحيحة، تبين بوضوح ودقة طبيعة الثغرات الأمنية، وتحديات الاعتمادية بجميع فئاتها ومصادرها، سواءً الناتجة عن الكوارث الطبيعية، أو التي يسببها الإنسان بقصد أو دون قصد. كما يجب الاهتمام بواقع العالم، وعدم الاعتماد على التنظير، المبني على النظريات، التي لا تأخذ في الاعتبار حقيقة البيئة الآنية، التي تعمل فيها البنية التحتية وشبكاتها. لقد اتضح أنه من الضروري تطبيق منهجية مدروسة، يمكن من خلالها فهم المشكلة، والبحث عن حلول

عملية، تؤدي إلى تحقيق اعتمادية يقبلها المجتمع والدولة، مع تحقيق موازنة بين التكلفة والأداء، وأهداف الاعتمادية، من خلال معالجة علمية دقيقة للتحليلات، والمقايضة بين الحلول المتوافرة، المبنية على معرفة تامة بجميع الحالات والنتائج المتوقعة.

ومع إدراك أنه لا يمكن القضاء على جميع المخاطر المتعلقة بتهديدات البنية التحتية؛ فإن كل ما يمكن فعله، هو تأكيد الحاجة لإنشاء إدارة فاعلة للمخاطر والأزمات، وجعلها على درجة مقبولة، على مستوى الدولة والمجتمع، تكون مهمتها دراسة مشكلة الاعتمادية، وتشمل: تطوير مفهوم تحليلي عن الاعتمادية المتوافرة ـ(الثغرات الأمنية ـ وبيئة التهديدات)ـ وإنشاء نظام إجراءات يتعامل مع الاعتمادية كعناصر أساسية، وتبني التزام الحذر واليقظة، وإجراءات التعليم المستمر لدعم الاعتمادية.

إن جميع آليات السياسات والتشريعات التقليدية، التي تفرضها الدولة للعمل في القطاعات الحكومية والخاصة، لتحقيق الأهداف الوطنية، بما في ذلك التشريعات، والأنظمة، والتراخيص، وفرض الرسوم، وغير ذلك من الأمور التي يمكن للدولة فرضها، يعطي بدائل مهمة في مضمار الاعتمادية؛ إلا أنه لن يكون لأي منها أي تأثير، ما لم يكن هناك إجماع يوضح الحد الأدنى للاعتمادية المقبولة، على المستوى الوطني، ويحدد التهديدات والمخاطر المقبولة، ويبين بوضوح الإجراءات الواجب تطبيقها، وتوعية المجتمع بهذه المخاطر الأمنية، وتبيين طرق الوقاية والعلاج، وتوفير الأموال والتكاليف، وتحديد الجهة المسؤولة عن التكاليف، هل هي الدولة بمفردها؟ أم أنها شراكة مع القطاع الخاص بصفته المستفيد الأول من البنية التحتية؟.

لقد استثمرت الدول كثيراً في مجالات متعددة أعطتها قدرات هائلة يمكن تطبيقها، لتحديد وتصنيف تحديات الاعتمادية. فهي تستطيع عن طريق إداراتها المختلفة، التنبؤ بتقلبات الطقس، وتوقع حصول الكوارث الطبيعية، وتجميع المعلومات الاستخباراتية، المتعلقة بتهديدات المخربين والإرهابيين، وتسهم إلى حد كبير في توضيح تحديات الاعتمادية، لصنَّاع التقنية والقطاع الخاص. لذا؛ فإنه من الضروري توفير ما لدى الدولة من معلومات، بصورة آنية وفورية، أثناء وقبل الأحداث، لمراكز التحكم في الشبكات الخاصة والحكومية، وجعل تلك المراكز مصادر فاعلة للإنذار الاستراتيجي المبكر، مع توفير الوسائل التقنية والتشريعية

لتحليل البيانات الواردة من جميع المصادر والجهات وتصنيفها بطريقة ملائمة، ووضعها موضع التنفيذ، ولا شك أن ذلك يتطلب اهتماماً طويل الأمد من الدولة والقطاع الخاص والمجتمع بأكمله.

إن على الحكومة والقطاع الخاص، التركيز على التطوير المشترك للمقاييس والمعايير التقنية، وطرق القياس والتصديق على الاعتمادية، فالتقنين مقبول بصورة عامة لدى الجميع، وقد يكون التصديق على مستوى الاعتمادية من قبل هيئات معتمدة من القطاعين الحكومي والخاص، طريقة ملائمة لتوضيح مستوى الاعتمادية القابلة للتطبيق على مجال واسع، الأمر الذي يساعد الشركات لتعزيز اعتماديتها، ويمكنها من اختيار مقايضات مبنية على معلومات موثقة. كما أن التصديق على مستويات الاعتمادية، يساعد على بناء ثقافة الاعتمادية لدى المجتمع التقني. ومن الضروري توعية مدراء الأنظمة والمسؤولين في الجهات المختلفة بالمخاطر الأمنية المتنوعة، وتحديد آلية واستراتيجية واضحة ومدروسة بعناية لتطبيقها عند حدوث أي من تلك المخاطر. كما أن لائحة القوانين العلمية، والمعايير المتفق عليها، المتعلقة بتصاميم الشبكات، وإنشائها مثل أنظمة الإنشاءات الكهربائية، والأنظمة المعمارية والإنشائية تقلل من خطر الأنظمة ذات الاعتمادية المنخفضة. ومن الضروري توافر فحوصات مقننة للاعتمادية، وشهادات مصدقة للمنتجات، الأمر الذي سيكون له قيمة عالية كوحدة قياس لمقارنة المنتجات والمعدات والأدوات المستخدمة في البنية التحتية.

وبما أن البنى التحتية مترابطة إقليمياً وعالمياً؛ فإنه من الضروري تعزيز التعاون الدولي، لأن فشل بنية تحتية مهمة في بلد ما، سوف يكون له تأثير كبير على معظم دول العالم، لاسيما وأن قطاعات الاقتصاد والصناعة العالمية، وقطاع المواصلات، وخاصة الجوية منها، مترابطة مع بعضها، لذلك فإن التعاون والتنسيق الدولي وتبادل المعلومات الأساسية المتعلقة بتعزيز الاعتمادية يعد أمر في منتهى الأهمية. وأخيراً وليس آخراً؛ فإن إنفاق الدولة في مجالات العلوم التقنية، والبحوث والتطوير، المتعلق بالاعتمادية، يمثل قضية في غاية الأهمية، في عصر المعلومات. فالإنفاق والاستثمار المستمر في مجالات اكتشاف ومكافحة الاختراقات، وتعزيز البنية التحتية الصلبة، والاتصالات المؤمنة، والاهتمام بجميع المجالات الحساسة، سيضيف الكثير إلى تقوية وتعزيز الاعتمادية، وتعد تهديدات البنية التحتية تحديات مشتركة بين عدد من الوزارات والهيئات والمنظمات في أي بلد ففي المملكة العربية السعودية ـ على سبيل المثال

ـ يكون لكل من وزارة الدفاع، والداخلية، والاستخبارات العامة، ووزارة تقنية المعلومات والاتصالات، وهيئة تقنية المعلومات والاتصالات، ومدينة الملك عبدالعزيز للعلوم والتقنية، علاقة مشتركة بصورة مباشرة لمعالجة التهديدات، مما يجعل الحاجة ماسة لتوضيح المسؤوليات وتحديدها في كل ما من شأنه تعزيز اعتمادية البنية التحتية. وقد يكون من الضروري، إشراك جميع فروع الدولة الإدارية والتشريعية والقضائية والمالية في هذا الموضوع، وتطوير إجراءات محددة لتعاون الجهات المختلفة لمكافحة مثل هذا الخطر وغيره من الأخطار المتعلقة بتهديدات البنية التحتية. ومن المؤكد أن المؤسسات الحكومية والقطاع الخاص شركاء في هذا الأمر، وأن عليهم مسؤولية كبيرة لتوفير خدمات ذات اعتمادية عالية، بتكاليف معقولة تمكِّنها من مواجهة التحديات المتوقعة باستمرار وعلى وجه السرعة. وكذلك؛ فإنه ينبغي تطوير إجماع مشترك لإدراك المشكلة وتوفير حلول طويلة الأمد، وهذا يتطلب التزاماً مستمراً من صنَّاع التقنية، والمرافق العامة، والمجتمع، والحكومة، على جميع المستويات. وبهذا يمكن لجميع هؤلاء الشركاء ضمان الاعتمادية لأكثر البنى التحتية قدرات على مر التاريخ.

المصادر والمراجع

المصادر والمراجع

١. رابطة العالم الإسلامي، المجمع الفقهي (١٤٢٤هـ) الطبعة الثانية، قرارات المجمع الفقهي الإسلامي بمكة المكرمة من عام ١٩٧٧ إلى عام ٢٠٠٤م ، مكة المكرمة المجمع الفقهي.

٢. الشوبكي، د. محمود يوسف (أبريل ٢٠٠٧) مفهوم الإرهاب بين الإسلام والغرب (بحث مقدم إلى مؤتمر «الإسلام والتحديات المعاصرة») الرياض: كلية أصول الدين، الجامعة الإسلامية، في الفترة: ٢-٣/ ٤/ ٢٠٠٧م.

3. Richard, Dr. Van Atta (2005) Energy and Climate Change Research and the "DARPA Model" (Presentation) Washington: The Washington Roundtable on Science and Public Policy, National Press Club (November 3, 2005)

4. Benkler, Yochai (2006) The Wealth of Networks, New Haven and London: Yale University Press.

5. Internet Usage Statistics, Access Date, April 19, 2010 From: http://www.internetworldstats.com/stats.htm

٦. هيئة الاتصالات وتقنية المعلومات (٢٠٠٧م) ـ مشروع دراسة استخدامات الإنترنت في المملكة العربية السعودية ـ التقرير الشامل ـ التقرير النهائي للسنة الأولى ٢٠٠٧م، الرياض: هيئة الاتصالات وتقنية المعلومات.

7. Saudi internet, Access Date, May 3 2008 From: http://www.internet.gov.sa/learn-the-web-ar/guides-ar/internet-in-saudi-arabia-ar\

8. United States Government Accountability Office GAO, (September 1996), Information Security Opportunities for Improved OMP Oversight of Agencies practices GAO/AIMD-96-110 .Washington: GAO.

9. NATO Parliamentary Assembly SUB-COMMITTEE ON THE PROLIFERATION OF MILITARY ECHNOLOGY, (April 2001) TECHNOLOGY AND TERRORISM International Secretariat Michael MATES (United Kingdom): April 2001

10. Marcel Dekker, Froehlich/Kent Encyclopedia of Telecommunications Volume 15, (1997) New York

11. Wood, J. Bradley & Schude, Gregg (2000) Modeling Behavior of The Cyber – Terrorist, SRI International Computer Science Laboratory Albuquerque: NM, USA

12. National Counterterrorism Center NCTC, Office of the Director of National Intelligence, (30April 2009), 2008 Report on Terrorism, Washington DC 20511: NCTC

13. Don Tapscott & Anthony D. Williams, (2006) Wikinomics: How Mass Collaboration Changes Everything, New York, Penguin Group.

14. Creative Commons Access Date, Feb 29, 2010 Home GNU General Public License, From: http://creativecommons.org/licenses/GPL/2.0/

15. Salone Home Page Interview of Eric S. Raymond Access Date Jan 10 2010 http://www.salon.com/?source=refresh

16. Raymond, Eric Access Date, Feb 29, 2010 Home Page, http://www.catb.org/~esr/faqs/hacker-howto.html

١٧. الماوردي، منير (١٤٢٨هـ) جريدة الشرق الأوسط الصادرة بتاريخ الأحد ٧ رجب ١٤٢٨ هـ ٢٢ يوليو ٢٠٠٧ العدد ١٠٤٦٣، شركات أميركية تستضيف الإرهاب الإعلامي على الإنترنت بأسعار زهيدة.

18. Golumbic, Martin Charles (2008) Confronting terror online Miami Heralds Sep. 10, 2008

19. Congressional Research Service [CRS], Affairs and National Defense

Division. (1997) Terrorism. The Media. And The Government Washington: CRS

20. Committee on Foreign Relations United State Senate. (JULY 26. 2007) One Hundred Tenth Congress First Session. Extraordinary Rendition. Extraterritorial Detention & Treatment of Detainees. WASHINGTON: U.S. Government Printing office (2008)
21. Department of Stat USA. Office of the Coordinator for Counterterrorism. Philip C. Wilcox. Jr. (1996). Patterns of Global Terrorism. Washington: Office of the Secretary
22. World Press Freedom Review Access Date. (May 3 2009) From: http://www.freemedia.at/publications/world-press-freedom-review/
23. Wikipedia. the free encyclopedia Access Date. (May 3 2010). From: http://en.wikipedia.org/wiki/Roman_roads
24. Independent System Operator ISO (January 8. 2004) Interim Report August 14. 2003 Blackout. Washington: ISO

٢٥. مكاتب عكاظ الداخلية، قضية اليوم (١٨/ ٦/ ١٤٢٨ الموافق ٣ يوليو ٢٠٠٧م)، جريدة عكاظ العدد ٢٢٠٧، توفير ألف ميجاوات تحسباً لانقطاع التيار- كهرباء الصيف. أعطال مفاجئة وأجواء ملتهبة.

26. Carnegie Mellon University. Software Engineering Institute. (January 1997). Report to the President's Commission on Critical Infrastructure Protection . Pittsburgh PA 15213: CMU.

٢٧. وكالة الأنباء السعودية (واس) السبت ١٨ ذي الحجة ١٤٣٠هـ - ٥ ديسمبر ٢٠٠٩م، جريدة الرياض العدد ١٥١٣٩، ضحايا كارثة جدة ١١٣ شهيداً وشهيدة.

28. Robb. John (2007) Brave New War. Hoboken. New Jersey: John Wiley & Sons

٢٩. سي. إن. إن. CNN (الأحد، ١١ ابريل ٢٠١٠) شريف موبلي.. اجتياز الاختبارات الأمنية للعاملين في المحطات النووية في العام ٢٠٠٨

30. Adilson E. Motter. and Ying-Cheng Lai (20 December 2002) Cascade-based attacks on complex networks (Study) Department of Mathematics. Center for Systems Science and Engineering Research. & Departments

of Electrical Engineering and Physics, Arizona State University, Tempe, Arizona.

31. سعيد، إدوارد، (٢٠٠٩) الثقافة والمقاومة ـ حاوره ديفيد بارساميان، ترجمة: علاء الدين أبو زينة ، بيروت: دار الآداب.

32. GAO Stings Nuclear Agency; Obtains License to Buy Radioactive Materials, Access Date, (July 11, 2007).

From: http://blogs.abcnews.com/theblotter/2007/07/goa-stings-nucl.html

33. اللواء التركي وزارة الداخلية السعودية (١٤٢٨هـ)، جريدة الشرق الأوسط الصادرة الثلاثاء ٢٥ صفر ١٤٢٩ هـ، ٤ مارس ٢٠٠٨ العدد ١٠٦٨٩ خلية الحج الإرهابية تابعة للقاعدة.. وزعيمها مزكّى من الظواهري صوتياً.

34. كمال قبيسي (١٤٢٢هـ) جريدة الشرق الأوسط الصادرة السبت ٠١ رمضان ١٤٢٢ هـ، ١٧ نوفمبر ٢٠٠١ العدد ٨٣٩٠ ، العثور على الجزء الحادي عشر من موسوعة الإرهاب * قتل طبيبين عربيين كانا يصنعان سماً قاتلا للاغتيالات * جمعية خيرية إسلامية شحنت ٣ مختبرات من أوكرانيا.

35. Smith, Pamela Ann (Mar 1, 2010) BUSINESS: FINANCIAL MARKETS; Gulf Cooperation Council (Article), London: The Middle East Magazine (1/3/2010)

36. Chivers, C.J. (January 22, 2006) Pipeline blasts cut Georgia gas supply, The New York Times.

37. United States General Accounting Office GAO (May 1996) Information Security, Computer Attacks at Department of Defense Pose Increasing Risks, Report to Congressional Requesters GAO/AIMD-96-84, Washington: GAO

38. U.S.-Canada Power System Outage Task Force, (April 2004), Final Report on the August 14, 2003 Blackout in the United States and Canada. USA & Canada

39. منتدى الرياض الاقتصادي، نحو تنمية اقتصادية مستدامة، (٤ ديسمبر ٢٠٠٧ م ـ ٢٤ ذو القعدة ١٤٢٨هـ، الموافق ٢ ـ٢٢)، (ورقة مؤتمر)، نحو تنمية مستدامة للبنية التحتية، الرياض ـ قاعة الملك فيصل للمؤتمرات.

40. Raphael F. Perl (2001). Terrorism, the Future, and U.S. Foreign Policy (Study) Washington: Foreign Affairs, Defense, and Trade Division, CRS Issue Brief for Congress updated September 13, 2001

الملاحق

ملحق ١

المواقع التالية تحتوي على مجموعة كبيرة من الصفحات تهتم بمواقع القراصنة وشئونهم:

موقع مجموعة جوجل للقرصنة:

- http://www.google.com/Top/Computers/Hacking/ هذا الموقع يحتوي على كم هائل من مواقع القرصنة وهو يستخدم كوسيلة إبلاغ عن المواقع المشبوهة للقراصنة.

- موقع مجموعة ياهوو للقرصنة:

- وهو شبيه بموقع مجموعة جوجل http://dir.yahoo.com/computers_and_/internet/security_and_encryption/hacking/Organizations/

- موقع المعاكس المتصل http://www.antionline.com/

- موقع ثقافة الشبكة http://w2.eff.org/Net_culture/Hackers/

- موقع تاريخ ثقافة القرصنة البريطاني http://bak.spc.org/dms/archive/britphrk.txt

أما المواقع التالية فهي توفر أرشيف لمواقع قرصنة تم توقيفها:

- موقع ٢٦٠٠ صفحة تم اختراقها http://www.2600.com/hacked_pages/

- موقع منظمة الاحتكاك /http://www.attrition.org/mirror/attrition
- موقع جالارى قرصنة الشبكات العنكبوتية Hysteria.sk hacked www gallery
- موقع المشروع «جاما»projectGama.com
- موقع جذور مؤمنة تحت الأرض/http://www.secureroot.com/category/ hackers/hacked_websites//

ملحق ٢

قائمة المصطلحات وتعريفاتها

ملحوظة: في متن الكتاب وفي هذه القائمة كلمة "نمط"= بروتوكول باللغة الإنجليزية Protocol

١ . شبكات الحواسيب Computers Networks

هي مجموعة من أجهزة الحواسيب والأجهزة الطرفية (كالطابعات والماسحات)، التي تتصِّل ببعضها سلكياً أو لاسلكياً.

٢ . الشبكة المحلية Local Area Network (LAN)

هي شبكة حواسيب متصلة ببعضها موجودة في موقع جغرافي واحد (مكتب أو مبنى).

٣. الشبكة الواسعة Wide Area Network (WAN)

هي شبكة حواسيب موزَّعة في مواقع جغرافية متعددة (عدة مبانٍ أو مُدُن)، وقد تتكوَّن الشبكة الواسعة من مجموعة من الشبكات المحلية، أو من أجهزة حواسيب ونهايات طرفية موزَّعة في أكثر من مكان، أو من مجموعة من الاثنين معاً.

٤. شبكات الإنترنت Internet

الإنترنت عبارة عن توصيل أنظمة الشبكات، التي تمكن الحواسيب من التواصل الآلي باستخدام نمط الاتصال TCP /IP، وقد تسببت الإنترنت في ولادة الشبكة العنكبوتية العالمية. وقد تم تطوير الإنترنت من برنامج أربانت **ARPANET** التابع لوزارة الدفاع الأمريكية، الذي تم تطويره في الستينات والسبعينات.

٥. شبكات الإنترانت Intranet

هي شبكة مملوكة لهيئة أو مؤسسة تستخدم تقنيات الإنترنت المختلفة، مثل المتصفحات web browsers ومزوِّدات الويب web servers في التعامل مع المعلومات وإنجاز مهام العمل داخل المؤسسة. ويمكن استخدام تقنيات تصميم الصفحات الخاصة بالإنترنت لعمل الوثائق والمستندات وخطابات العمل الخاصة بالشركة وتبادلها بين العاملين، عن طريق تصفحها، من خلال المزوِّد الرئيس لموقع الشركة. ويمكن أيضا تصميم قواعد بيانات Data Bases خاصة بالشركة ووضعها على مزوِّد الموقع Web Server لضمان الوصول إليها من أي مكان داخل أو خارج الشركة للعاملين في الشركة أو المؤسسة دون سواهم، مع تحديد الصلاحيات المختلفة للعاملين وتحديد مستويات الحماية والأمن Security Level، كما يمكن تبادل البريد الإليكتروني وعمل دليل إليكتروني يحوي كل بيانات الأشخاص، الذين يعملون في المؤسسة.

٦. الشبكة العنكبوتية العالمية World Wide Web (WWW)

هي مجموعة الوثائق المخزنة في الحواسيب المنتشرة في الفضاء العالمي، وتستخدم نمط التشعيب HTTP. وتمكن الوصول إلى هذه الوثائق من خلال متصفح الشبكة Browser بالإضافة إلى التنقل بين الصفحات باستخدام روابط تطبق لغة HTML. وباختصار؛ فإنه يمكن تعريف الشبكة العنكبوتية بأنها: الشبكة، التي توصل الحواسيب بالصفحات والملفات التي تعود المجتمع على تصفحها.

٧. نمط التحكم بالإرسال Transmission Control Protocol (TCP)

نمط التحكم بالإرسال TCP هو نمط مخصص لنقل البيانات **Transport Protocol**،

وهو يوفر اتصالاً موجها Connection- Oriented ويدعم اتصالاً مزدوج الاتجاه Full Duplex ويوفر تحكماً لتدفق البيانات.

٨. نمط الإنترنت Internet Protocol (IP)

نمط الإنترنت IP هو عبارة عن نمط شبكة Network Protocol، وهو يوفر تسليم البيانات دون اتصال مسبق Connectionless.

٩. باقة نمط التحكم بالإرسال/ نمط الإنترنت Transmission Control Protocol /Internet Protocol (TCP/IP)

يعد النمط القياسي المستخدم، لضمان التوافق بين الأنواع المختلفة من الأجهزة، والشبكات وأغلب الشبكات المحلية والواسعة تدعم هذه الباقة من الأنماط، وهو يتكون من مجموعة أنماط تحكُّم تسمح للشبكات و الأنواع المختلفة من الأجهزة بالاتصال فيما بينها، وتوفر خصائص تشبيك و توجيه ووصول لشبكة الإنترنت والاستفادة من مواردها. وقد طورت أساسا في عام ١٩٦٩م من قبل وكالة مشاريع البحوث المطورة للدفاع الأمريكي.

١٠. نمط الاتصال في تام Virtual Telecommunications Access Method (VTAM)

برنامج تطبيقي أنتجته شركة آي بي إم IBM يوصل المستخدمين بأدوات ومعدات الاتصال، وهو من أوائل البرمجيات، التي مكّنت المبرمجين من التعامل مع الأدوات كوحدات منطقية Logical Units دون الحاجة لفهم تفاصيل وأنماط الخطوط الموصلة أو الناقلة وأطر تشغيل الأدوات.

١١. نمط توصيف النصوص التشعيبي لنقل البيانات HyperText Transfer Protocol (HTTP)

وهو مجموعة من القواعد تستخدم لنقل الملفات (النصية والرسومات والصور والصوت والصور المتحركة وجميع الوسائل المتعددة) من خلال الشبكة العنكبوتية

وشبكات الإنترنت، والإنترانت، وهو برنامج تطبيقي يعمل كطبقة فوق نمط /TCP) .IP)

١٢. لغة توصيف النص المتشعب HyperText Markup Language (HTML)

هي لغة برمجة تستخدم في وصف هيئات النصوص التشعيبية Hypertext، ويمكن تطبيقها باستخدام برامج شبيهة بمعالجات النصوص العادية. وتستخدم لغة HTML في إعداد صفحات شبكات الإنترنت والشبكة العنكبوتية.

١٣. الرابط Link

هو رابط تشعيبي يمكن اختياره من قبل المتصفح، للوصول إلى معلومة أو وثيقة أو أي من الوسائل المتعددة، وهو يتكون من كلمة أو أكثر أو صورة أو رمز.

١٤. التشعيب النصي HyberText

هو تنظيم للمعلومات والوثائق، بحيث تكون متصلة ببعضها حسب رغبة المحرر، ويمكن الوصول إلى أي منها بالضغط على الرابط المخصص لذلك.

١٥.الارتباط التشعيبي Hyperlink

عبارة عن مجموع للاصطلاحين Link و HyberText

١٦. النهايات الطرفية Terminals

النهايات الطرفية هي الأجهزة والمعدات المتصلة سلكياً أو لاسلكياً بشبكة الحواسب من شاشات وطابعات وموجهات وأجهزة الإدخال، مثل الفأرة ولوح المفاتيح Key Board، وتتصل مع الأنظمة المساندة عن طريق نمطي الاتصال TCP/IP أو VTAM، بهدف نقل وتبادل المعلومات بين الحاسب الآلي والنهايات الطرفية المتصلة به في إطار النقل على الخط المباشر On line للبيانات. وتقوم شبكة الإنترنت بالربط بين النهايات الطرفية Terminals للحاسبات باستخدام إحدى قنوات الاتصال.

١٧ . مزوِّد ويب Web Server

عبارة عن برنامج حاسوبي يوفر خدمات ومحتوى، مثل (الصفحات البيتية)، باستخدام نمط تناقل النصوص التشعيبية HTTP من خلال الشبكة العنكبوتية، و يسمى أحياناً مزوِّد الشبكة، وهو يصف أيضاً الحاسوب الذي يشغل البرنامج.

١٨ . عرض الحزمة Band Width

مقدار حركة مرور البيانات، التي يمكن استيعابها في لحظة واحدة، ووحدة قياسها "بت في الثانية".

١٩ . مزوِّد خدمة المعطيات Data Service Provider (DSP)

هي الشركات والمؤسسات المرخص لها من قبل هيئة الاتصالات وتقنية المعلومات بتقديم خدمات البيانات في المملكة، بما في ذلك البوابات الرئيسة، التي يتم المرور عبرها إلى شبكة الإنترنت العالمية. وقد بلغ عدد المزوِّدين المرخصين لخدمة المعطيات على نطاق تجاري في المملكة في صيف ٢٠٠٦م ثلاثة مزوِّدين فقط.

٢٠ . مقدمي خدمات الإنترنت Internet Providers (IP) و تسمى أيضاً مزوِّد خدمة الإنترنت Internet Service Providers (ISP)

هي الجهة، التي تربط عملاءها ـ سواء الشركات أو الأفراد ـ بشبكة الإنترنت عن طريق مزوِّدي خدمة المعطيات DSP المرخص لهم من قبل الجهة المخولة لذلك، مثل (هيئة الاتصالات وتقنية المعلومات).

٢١ . اسم نطاق Domain Name

اسم يشير إلى الحيز الذي تملكه مؤسسة معينة في فضاء الإنترنت، ويمكن ترجمته إلى عنوان معين في الشبكة، مثل: orgnization.com، وتتألف أسماء النطاقات من مقطعين أو أكثر تفصل فيما بينها علامة النقطة «.»، وفيما عدا المواقع الأمريكية، يبدأ اسم النطاق (من أقصى اليمين) بحرفين يدلان على اسم البلد، بينما يدل المقطع التالي على تصنيف المؤسسة؛ فالحروف com تشير إلى مؤسسة تجارية commercial، والحروف gov تشير إلى مؤسسة

حكومية government، و edu على مؤسسة تعليمية. وهكذا. وتخلو أسماء النطاقات الأمريكية من المقطع الدال على الدولة التي ينتمي إليها النطاق. ولتلافي تعارض أسماء النطاقات، كلفت مراكز Network Information Centers NICs بتسجيل أسماء النطاقات، ويقع على عاتقهما ترجمة هذا الاسم إلى عنوان رقمي في الشبكة.

٢٢. عنوان إنترنت Universal Resource Locator (URL)

عنوان لوثيقة أو ملف أو موقع على الإنترنت، والـURL، ليس الشيء نفسه كاسم النطاق الذي يكون جزء من عنوان الإنترنت.

٢٣. عنوان نمط الإنترنت IP Address

لكل جهاز حاسوب موصول بالإنترنت عنوان يسمى «عنوان نمط الإنترنت»، ويكون هذا العنوان على هيئة أربعة أعداد مفصولة عن بعضها بنقاط، ومثال ذلك ١٢٣,٤٥,٦٧,٨٩

٢٤. نمط حل العناوين Address Resolution Protocol (ARP)

هو النمط الذي يترجم عناوين الإنترنت الرقمية، مثل العنوان (٤٢,٣,١٠,١٢٨)، إلى عناوين حرفية في الشبكة، ويعد ARP أحد عناصر طاقم النمط الشهيرة TCP/IP، وهو يلعب دوراً أساسياً في تلمس حزم البيانات، المرتحلة عبر الإنترنت، لطريقها باتجاه أهدافها، طبقاً للعنوان الذي تحمله.

٢٥. خدمة أسماء النطاقات DNS Domain Name Service

عبارة عن قاعدة بيانات فورية تستخدم في المطابقة بين العناوين الرقمية لنمط الإنترنت مثل: (٤٢,٣,١٠,١٢٨)، والأسماء الحرفية للنطاقات، التي يسهل على الناس قراءتها وتذكرها مثل: Organization.org ولا تجتمع بيانات DNS في كمبيوتر واحد معين، بل هي موزعة بين آلاف مزوِّدات DNS المنتشرة عبر شبكات الإنترنت.

٢٦. شبكة وزارة الدفاع الأمريكية

US Defense Advanced Research Projects Agency (DARPA).

وكالة مشاريع البحوث المطورة للدفاع الأمريكي، وقد استخدم في البداية لبناء شبكة مشاريع البحوث المطورة للدفاع الأمريكي Advanced Research Projects Agency Network (ARPANET)، وهي عبارة عن شبكة كانت تربط بين أربع جامعات أمريكية تجري بحوثاً في مجال الدفاع.

٢٧. الموجِّه Router

هو جهاز يتألف من مجموعة من الأدوات والبرامج، يستخدم لربط شبكتين أو أكثر من الشبكات الفرعية المختلفة بواسطة إشارات سلكية أو لاسلكية، وكثيراً ما يستخدم في الشبكات الواسعة، مثل الإنترنت والإنترانت، ومهمته الأساسية توجيه حزم التراسل للشبكة المراد التواصل معها.

٢٨. التوجيه الديناميكي Dynamic Rerouting

هي شبكة عالمية تربط الملايين من أجهزة الكمبيوتر بعضها ببعض، حيث تقوم أجهزة الكمبيوتر هذه بإرسال واستقبال المعلومات باستخدام نمط الإنترنت (IP) الذي هو عبارة عن "لغة" تمكن أجهزة الكمبيوتر من فهم بعضها البعض.

٢٩. نظام أمن الاتصالات Secure Sockets Layer (SSL)

عبارة عن نمط طورته شركة نتسكيب Netscape، لبعث الوثائق الخاصة عن طريق الإنترنت، ويستخدم نظام تشفير خاص بمفتاحين لتشفير البيانات، أحدهما مفتاح معلن يعرفه الجميع، والآخر مفتاح سري يعرفه المستقبل فقط، ومعظم المتصفحات لحديثة تدعم هذا النمط. ويطلق عليه أحياناً (TLS) أو نظام أمن النقل، وهما نمطان يهدفان لمحاولة ضمان سلامة وأمن البيانات على الإنترنت.

٣٠. متصفح الشبكة Browser

متصفح الشبكة، هو برنامج يمكن المستخدمين من التصفح والتعامل مع المحتوى في

الصفحات البيتية مثل النصوص والصور والفيديو والموسيقى والألعاب الإلكترونية، أو أي مواد أخرى متوافرة في الصفحات والمواقع الإلكترونية. وهي الوسيلة الشائعة، التي يستخدمها مجتمع الإنترنت لتصفح مواقع الشبكة العنكبوتية العالمية. وفي الغالب؛ فإن هذه المحتويات تكون مخزنة في مزوِّدات الشبكة، وتعرض النصوص والصور على شكل صفحة في موقع على شبكة الإنترنت أو في شبكة محلية، و يمكن أن تحوي روابط لصفحات أخرى في الموقع نفسه أو في مواقع أخرى، وتتيح للمستخدم أن يصل إلى المعلومات الموجودة في المواقع بسهولة وسرعة عن طريق تتبع الروابط، وهناك العديد من المتصفحات المشهورة مثل مايكروسوفت إنترنت، وإكسبلورر، وموزيلا، وفايرفوكس، وسفاري وجوجل كروم، وأوبرا.

٣١. الهيئة الرقمية Digital Form

هي صيغة تطلق على أي وثيقة أو صورة تم تحويلها إلى رموز يمكن تخزينها في أي وسط الكتروني ويمكن استرجاعها وطباعتها أو إرسالها عبر وسائل الاتصالات ونقل المعلومات المتوافرة.

٣٢. الأسواق التقليدية Markets

هي الأسواق العادية التي تخضع لملكية خاصة يتحكم فيها الأفراد والهيئات والمؤسسات والشركات، ويتم المقايضة فيها بصورة مباشرة بين البائع والمشتري، وتخضع لقوانين البيع والشراء المعتمدة.

٣٣. الأسواق الافتراضية Non-Markets

هي أسواق تعتمد في البيع والشراء على شبكات الإنترنت، وأهم مميزاتها أنها لا تخضع للملكية الخاصة، وهي محصلة تعاون اجتماعي غير منسق وبدون التزام من المشاركين في الإنتاج. ويتم البيع والشراء من خلال شبكات الإنترنت العالمية، كما أن الدفع عن طريق بطاقات الإئتمان بواسطة برامج دفع مؤمنة ومشفرة.

٣٤. وحدة المعالجة المركزية Central processing unit (CPU)

يطلق عليها اختصاراً المعالج (Processor) وهي أحد مكونات الحاسوب الرقمي

التي تقوم بتفسير التعليمات ومعالجة البيانات التي تتضمنها البرمجيات. ويعد المعالج بالإضافة للذاكرة الرئيسة ووحدات الإدخال والإخراج من أهم مكونات الحواسيب الدقيقة (Microcomputers) الحديثة، وتعرف المعالجات التي تم تصنيعها بواسطة الدوائر المجمعة (Integrated circuits) بالمعالجات الدقيقة (Microprocessor)، والتي بدأ تصنيعها منذ منتصف سبعينات القرن العشرين على شكل رقائق مدمجة حلت محل معظم أنواع المعالجات الأخرى. ويدل مصطلح وحدة المعالجة المركزية على فئة من الأدوات المنطقية، التي تقوم بتنفيذ برامج حاسوبية معقدة.

٣٥. الإنتاج الجماعي Social Production

هو إنتاج للمعلومات من خلال شبكات الإنترنت، يتميز باللامركزية والتعاونية واللاملكية المبني على المشاركة في الموارد و المخرجات بين عدد كبير من الأفراد المنتشرين على نطاق واسع ومتصلين بدون قيود، يتعاونون مع بعضهم دون الاعتماد على إشارات تصدر من الأسواق أو أوامر المدراء.

٣٦. الحكومة الإلكترونية Electronic Government

هي تسهيل سبل أداء الإدارات الحكومية لخدماتها العامة باستخدام التطورات التقنية في مجالات تقنية صناعة المعلومات، مثل الإنترنت والتقنيات الرقمية الأخرى، بهدف تقديم تلك الخدمات والمعلومات للمواطنين بأشكال وسبل جديدة سهلة وسريعة، تختلف عن شكلها الروتيني التقليدي إلى أشكال جديدة إلكترونية باستخدام الحاسب الآلي عبر شبكة الإنترنت وشبكات الاتصال، مما يستلزم تطويراً للبنية الإدارية والفنية لتلك الإدارات، وتغييراً في أنظمتها التشريعية.

٣٧. التعاملات الإلكترونية Electronic Interactions

هي تبادل المعلومات بين الحواسيب، وتكون في العادة عن طريق الإنترنت، ويستخدم هذا الاصطلاح أحياناً كرديف للحكومة الإلكترونية.

٣٨. التجارة الإلكترونية e-Commerce

هي تنفيذ بعض أو كل المعاملات التجارية في السلع والخدمات، التي تتم بين جهة تجارية وأخرى أو بين مستهلك وجهة تجارية باستخدام تقنية المعلومات والاتصالات، وتشمل بيع وشراء البضائع والخدمات والمعلومات من خلال استخدام شبكة الإنترنت حيث يلتقي البائعون والمشترون والسماسرة عبر الإنترنت من خلال المواقع المختلفة لعرض السلع والخدمات والتعرف عليها والتواصل والتفاوض والاتفاق على تفاصيل عمليات البيع والشراء. كما يتم من خلال الإنترنت أيضاً دفع ثمن الصفقات من خلال عمليات تحويل الأموال عبر بطاقات الائتمان أو غيرها من وسائل الدفع الإلكتروني. كما يمكن أيضاً الجمع بين وسائل التجارة الإلكترونية والتقليدية في آن واحد، من خلال القيام بجزء من الإجراءات في الوسط الإلكتروني، مثل الاتفاق على السعر والكمية واستكمال ما تبقى من خلال الأنشطة الملموسة، مثل معاينة البضائع أو استلامها من مكان الشحن أو الدفع النقدي.

٣٩. الموانئ الإلكترونية Ports

الميناء في سياق الإنترنت والحواسيب يعبر عن المداخل والمخارج في أي آلة الكترونية لتوفير تبادل الإشارات والبيانات الإلكترونية بين الآلات، وهو نقطة تفاعل الحاسوب أو اتصاله بحاسوب آخر أو أي نهاية طرفية مثل الطابعات.

٤٠. الهندسة الاجتماعية Social Engineering

خداع استراتيجي شائع يهدف لخداع عامل مقسم المساعدة الفنية helpdesk في مؤسسة أو مرفق حكومي للحصول على معلومات سرية، مثل كلمات المرور، حيث يدعي المخادع أنه أحد المدراء وأنه نسي كلمة المرور الخاصة به ويريد الدخول على عجل لأمر مهم طلبه منه المدير العام وعليه إرساله له على وجه السرعة. كما أنه يطلق أحياناً، على عمليات الاصطياد fishing، التي يتبعها بعض القراصنة في خداع الأفراد لإرسال معلومات سرية، مثل اسم المستخدم وكلمات المرور.

٤١. كلمات المرور Pass Word (PW)

هي عدد معين من الأرقام والحروف والرموز الرقمية تستخدم لتعريف مستخدم محدد

للحاسوب، ليتمكن من التواصل مع نظام حاسوبي. وتعد كلمة المرور تأكيداً للتعريف بأن المتصل أو الشخص، الذي عرف نفسه بأنه هو فعلاً الشخص المعني وأنه صاحب الحساب الذي يرغب التعامل معه. وتأتي كلمة المرور مرتبطة باسم فريد يعرف بأنه اسم المستخدم وباللغة الإنجليزية «User Identification» أو ID، وهي معروفة للمستخدم والنظام فقط ويمكن تغييرها في أي وقت من قبل الشخص المالك لها.

٤٢. سبام SPAM

هي رسائل تكون في الغالب دعائية ترسل إلى عدد كبير من الناس وهي غير ذي فائدة لمستقبلها، ويستخدمها القراصنة لإغراق المواقع المستهدفة بالحركة المرورية، التي تؤدي إلى تعطيل الموقع.

٤٣. خلل BUGS

هو خلل في الترميز الأساسي لأي برنامج أو في طريقة عمله وتشغيله. وقد أخذ هذا الاصطلاح من حشرة البق، حيث أن هذه الحشرة تسببت في تعطيل نظام لمدة طويلة لم يستطيع الخبراء إعادته للخدمة إلا بعد وقت طويل، عندما اكتشفوا أن حشرة بق بنت بيتها في إحدى دوائره الإلكترونية، وتسببت في عمل دائرة تيار مقفلة كانت السبب في العطل.

٤٤. تعطيل الخدمة Denial of Service (DoS)

عندما ينجح شخص أو أكثر في منع مستخدم أو منظمة من استخدام خدمة أو مورد تكون في الغالب متوافرة لهم. ويؤدي تعطيل الخدمة إلى جعل شبكة محددة غير قادرة على مواصلة تقديم خدماتها. وهذا النوع من الهجوم لا يهدف لسرقة المعلومات، إلا أنه يتسبب في خسائر مادية عالية، كما أنه يمكن أن يتسبب في إفساد وتخريب الملفات والوثائق وبعض البرامج التطبيقية في الحواسيب. وتاريخاً تسبب هجوم منع الخدمة في إجبار مواقع مشهورة تخدم ملايين الأشخاص من التوقف عن تقديم خدماتها لمدة وصلت إلى أيام في بعض الحالات.

٤٥. أنظمة السمات الحيوية Biometrics

كلمة biometrics «القياسات الحيوية» من الكلمة الحيوية bio أي (الحياة life)

ومتري metric وكلاهما مقتبسة من اللغة اليونانية، وفي مجال تكنولوجيا المعلومات، على وجه الخصوص، فإن القياسات الحيوية تستخدم كشكل من أشكال إدارة الوصول للهوية identity access management ومراقبة الدخول access control. كما أنها تستخدم لتحديد هوية الأفراد في الجماعات الذين يكونون تحت المراقبة باستخدام خصائصهم الفسيولوجية والسلوكية مثل: الحمض النووي (DNA) ـ بصمات الأصابع ـ هندسة اليد أو الأصابع (Hand Geometry) ـ الوجه ـ بصمة العين (قزحية العين) ـ شبكية العين ـ مخطط الأوعية الدموية ـ التعرف على الصوت ـ التعرف على التوقيع (الإمضاء) ـ إيقاع حركة اليد في استخدام لوحة المفاتيح وأي من هذه الخصائص يمكنها تحديد هوية الشخص بشكل فريد، لتحل محل أو تكمل طرق الأمن التقليدية، من خلال توفير اثنين من التحسينات الرئيسة، وهي أن القياسات الحيوية الشخصية لا يمكن سرقتها بسهولة ولا يحتاج الشخص لحفظ كلمات السر أو الرموز. وتستطيع المقاييس الحيوية حل مشاكل مراقبة الدخول والغش والسرقة بشكل أفضل.

٤٦. **الهجوم القهري** Brute Force Attacks

الهجوم القهري هو أسلوب يعتمد على المحاولة والخطأ باستخدام برامج تطبيقية خاصة لمعرفة مفاتيح الشفرة، أو استحصال كلمات المرور من خلال جهود كبيرة ومحاولات مستمرة، دون الحاجة لاستراتيجيات فكرية وعقلانية.

٤٧. **نمط نقل الملفات** File Transfer Protocol (FTP)

عبارة عن إحدى تسهيلات TCP/IP التي تمكن من نقل الملفات بين الحاسوب والموقع المضيف على الشبكة، ومن ميزات FTP الرائعة أنها تقوم بترجمة هيئة الملفات النصية بطريقة أوتوماتيكية، حيث إن الحواسيب تعمل بنظم تشغيل مختلفة ونماذج Formats متعددة للملفات النصية، لذا؛ فإنه من الضروري تهيئتها، وهو ما يقوم به FTP، ويسمح هذا النمط بالدخول إلى أي موقع إلكتروني لإرسال أو استقبال ملفات من أي نوع. وفي العادة، يتم تزويد المواقع بالصفحات البيتية عن طريق نمط نقل الملفات أو نمط مشابه.

٤٨. قائمة المواقع المجهولة لنمط نقل الملفات Anonymous FTP Sites

عبارة عن نظام يمكن المستخدم من الوصول لوثائق مخزنة في المزوِّد، الذي يستضيف الموقع دون أن يكون له صلاحيات إدارية، أي أن المستخدم يمكنه الدخول إلى الحساب كـ«ضيف»، ولا داعي أن يعرف نفسه للوصول للملفات.

٤٩. نمط Tenet

هو أحد أنماط الإنترنت للتواصل مع مزوِّدات الإنترنت وبمجرد أن يتم الدخول للمزوِّد عن طريق هذا النمط، فإن المزوِّد يستجيب بتوفير سطر لإدخال الأوامر.

٥٠. حصان طروادة Trojan Horse

عبارة عن شفرة صغيرة يتم تحميلها لبرنامج رئيس من البرامج الشائعة، التي يكثر استخدامها، ويقوم ببعض المهام الخفية ، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو تقويضها ليسهل اختراق جهازه وسرقة بياناته. وسمي بهذا الاسم لتشابه عمله مع أسطورة حصان طروادة الخشبي، الذي اختبأ فيه عدد من الجنود اليونانيين، وكانوا سببا في فتح مدينة طروادة.

٥١. قاعدة بيانات من يكون www.who.is

هي قاعدة بيانات مجانية تحتوي على معلومات ملاك المواقع والصفحات البيتية في الإنترنت، ويمكن من خلالها الحصول على اسم مالك أو ملاك الموقع وأرقام هواتفهم، وبالنظر في مكان تسجيل الموقع المستهدف، يمكن معرفة أكبر قدر من المعلومات عن المالك للموقع وعن الشبكة والأشخاص المعنيين

٥٢. مواقع الإنترنت العامة Bublic Web Sites

هي مواقع في الإنترنت يمكن الدخول إليها وتصفحها باستخدام أي متصفح، وهو عكس الموقع الخاص الذي لا يستطيع الدخول إليه المتصفحون إلا بتصريح خاص.

٥٣. الأمر شل Command Shell

هو مصطلح بديل لنقطة تعامل أو تفاعل الحاسوب مع المستخدم، حيث إن أنظمة التشغيل والبرامج التطبيقية توفر طبقة أو درع Shell، بديل لتسهيل التعامل مع البرنامج.

٥٤. بادئة الرموز شل Meta-Characters Shell

كثير من الأنظمة مثل the command line shell and SQL interpreters تعد بعض الرموز المدخلة ليست ضمن البيانات المعتمدة، وهذه الرموز يمكن اعتبارها أوامر، أو أنها تحد البيانات من التعرف على الأوامر أو البيانات الأخرى. وأحد أهم مشاكل اختراقات هذه الرموز تأتي من بادئة رموز شل، لكونها تخزن في ملف يسمى (stored in /bin/sh) في نظام يونكس وغيره من البرامج المشابهة، وتفسر عدداً من الرموز على نحو خاص يمثل أوامر محددة يفهمها النظام، ويمكن أن تستخدم هذه الحقيقة لمهاجمة النظام والرموز المقصودة هي: ` ; &
< \ « | * ? ~ < > ^ ( ) [ ] { } $ \n \r

٥٥. مزوِّد سجلات الشبكة Server Logs

سجل أداء مزوِّد الشبكة، عبارة عن ملف أو عدد من الملفات يولدها مزوِّد الشبكة، لحفظ جميع الأنشطة والأعمال التي تجرى عليه، وفي الغالب؛ فإنه من الصعب الوصول لهذه الملفات من قبل مستخدمي الإنترنت العاديين، وهي تدار من قبل المسؤول عن أمن الموقع. ويستخدم التحليل الإحصائي لسجل الأداء لفحص نمط حركة المرور من حيث الوقت والتكرار والمستخدم وغير ذلك من وظائف الموقع.

٥٦. نظام كشف اختراقات الشبكة Network Intrusion Detection System (NIDS)

عبارة عن برنامج يستخدم لاكتشاف النشاط الهجومي المؤذي، مثل هجوم منع الخدمة أو هجوم استكشاف الموانئ، حيث يتولى النظام مراقبة وقراءة الحزم الواردة ومحاولة تحديد النمط المشبوه، الذي يسمى في العادة توقيع المهاجم. وعلى سبيل المثال، عندما يكتشف النظام طلبات كبيرة لعدد كبير من الموانئ، يمكن افتراض أن شخصاً ما يحاول استكشاف الموانئ العاملة في الحاسوب أو حواسيب الشبكة المستهدفة، ولا يقتصر عمل نظام كشف الهجوم أو

التسلل على الحزم الواردة بل يحاول مراقبة الحزم الصادرة لاكتشاف أي محاولات مشبوهة أو عدم التزام بتعليمات الأمن.

٥٧. طفح الذاكرة المؤقتة Buffer Overflow

يحدث طفح الذاكرة عندما يحاول برنامج أو معالج رقمي أن يخزن بيانات أكثر مما هو مسموح به في مستودع تخزين من مستودعات الذاكرة المؤقتة (The Buffer)، حيث إن مستودعات الذاكرة المؤقتة صممت لاستيعاب كمية محددة من البيانات، وهي البيانات أو المعلومات الإضافية، التي تخزن فيها لحين نقلها إلى وجهتها المقررة في البرنامج التطبيقي المراد تشغيله، وعند تجاوز سعة المستودع فإن البيانات الزائدة تنتقل أو تطفح إلى مستودع مجاور من مستودعات الذاكرة المؤقتة، مما يتسبب في إفساد المعلومات الموجودة في المستودع المجاور أو استبدالها بالمعلومات التي طفحت إليه.

٥٨. الهجوم على متصفح الشبكة web browser attack

ينشأ الهجوم على متصفح الشبكة من المواقع السيئة، ولكن نتيجة لبعض الثغرات الأمنية والترميز السيئ في البرامج الداعمة للصفحات البيتية. تمكن المهاجمون من اختراق عدد كبير من المواقع الموثوقية، حيث تمكنوا من إضافة برنامج صغير لا يؤثر على مظهر الصفحة البيتية ولكنه يوجه الزائر، دون أن يشعر إلى صفحة أخرى تقوم بتحميل برنامج خبيث لحاسوب المتصل، يمكن المهاجم (كاتب البرنامج) من التحكم في الحاسوب المستهدف وسرقة المعلومات الشخصية المتوفرة في الحاسوب وبالأخص معلومات بطاقات الائتمان.

٥٩. الذاكرة المخفية cache history

هي ذاكرة تستخدم في الحواسيب لتحسين مستوى الأداء، وذلك بتخزين البيانات، بحيث تكون في متناول المستخدم فور طلبها. والمعلومات، التي تخزنها هذه الذاكرة تكون في الغالب قيماً جرى التعامل معها مسبقاً، أو نسخاً لقيم أصلية تم تخزينها في مكان آخر. وبالمقارنة مع الذاكرة المؤقتة Buffer التي يتحكم فيها العميل بصورة كاملة؛ فإن الذاكرة المخفية Cache تخزن معلوماتها بصورة تلقائية ودون أي تدخل من المستخدم.

٦٠. الذاكرة المؤقتة The Buffer

هي ذاكرة مخصصة لاستيعاب كمية محددة من البيانات بصورة مؤقتة، لحين نقلها إلى وجهتها المقررة في البرنامج التطبيقي المراد تشغيله.

٦١. الجدار الناري Fire Wall أو الحاجز الناري Firewall

نظام أمني لتنظيم حركة المرور عند نقاط الاتصال بين الإنترنت والإنترانت (أو بين أي شبكتين بصورة عامة)، وهو يسمح لحزم البيانات بالعبور بين الشبكتين، أو يمنعها، اعتماداً على مجموعة من القواعد يحددها مدير الشبكة (مثل اسم المستخدم وكلمة السر، أو عنوان IP، أو رقم هاتف المتصل في حالة السماح بالدخول عبر اتصالات dial-in ...). ويوجد العديد من حلول الحواجز النارية، فبعضها عبارة عن برمجيات تعمل فقط مع مزوِّد خاص ، والبعض الآخر حلول متكاملة، تتألف من برمجيات تعمل على أجهزة مخصصة، وكانت الحواجز النارية تعمل في السابق، في بيئة يونيكس فقط، أما الآن فهناك العديد من الحواجز الفعالة، التي تعمل في بيئة ويندوز.

٦٢. أداة الطرق PING

عبارة عن أوامر تستخدم في الشبكات الحاسوبية لفحص ومعرفة إمكانية الوصول لمزوِّد الشبكة المضيف، أو فحص عنوان نمط الإنترنت، للتأكد من كونه مستخدم من عدمه. ومن الممكن معرفة سرعة الحاسوب ومدى سلامته ونمط الإنترنت المستخدم بهدف تحديد صحة الشبكة أو اتصال الإنترنت.

٦٣. المفوض (أو الوسيط) Proxy

المفوض، هو مزوِّد يوضع بين جهاز المستخدم والإنترنت. ويمكن أن يعمل بمثابة جدار ناري لتأمين الحماية، وكمنطقة ذاكرة مخفية (Cache) لتسريع عرض صفحة الويب وكمرشح للحيلولة دون وصول المستخدم إلى مواقع إلكترونية فيها مادة محظورة.

٦٤. كتل البيانات Datagram

وحدة قياس تستخدم في تنظيم حركة نقل نمط شحنة المستخدم User Datagram

Protocol (UDP)، وكل داتاجرام تمثل وحدة تراسل واحدة والثمانية بايت الأولى فيها تمثل المعلومات العلوية Header Information

٦٥. نظام الترشيح (Filtering)

يقوم نظام الترشيح بحجب وصول مستخدمي الإنترنت إلى المواقع الإلكترونية ذات المحتوى المؤذي والعدواني والإباحي.

٦٦. أداة «ميتاسبلويت Metasploit» المجانية

عبارة عن برنامج يمكن الحصول عليه مجاناً من الإنترنت، وهو سهل الاستعمال يستخدم لفحص الشبكات ومعرفة إمكانية الدخول إليها دون حاجة لتسجيل تعريف المستخدم وكلمة المرور.

٦٧. ثغرات نصوص المزوِّد الجانبية (SSC) Server-Side Scripts

هي ثغرات أمنية توجد في الغالب في بعض البوابات والموانئ العامة

٦٨. الواجهة العمومية للمعبر Common Gateway Interface (CGI)

وهي أداة تسمح بتطبيق برنامج في الخلفية لتنفيذ مهام لا يمكن إجراؤها باستخدام لغة توصيف النص المتشعب(HTML)، وهي وسيلة لنقل المعلومات، التي يدخلها المستخدم في النماذج forms التي توجد في الصفحات البيتية، إلى البرامج التي تعالجها في جهة ومزوِّد الشبكة، وبالعكس، لأن الصفحات البيتية لا يمكنها التعامل مباشرة مع القارئ. وقد كان من المستحيل للصفحات البيتية التعامل مع القارئ، إلا من خلال التعامل مع المزوِّد المستخدم من قبله إلى أن ظهرت مشغلة نصوص جافا JavaScript. ومشغلات النصوص هذه وغيرها من البرامج، هي التي تقوم بالتعامل باستخدام واجهة البوابة العامة لتوفير برنامج تفاعلي في الصفحة البيتية.

٦٩. نقل منطقة النطاق domain zone transfers

هو مصطلح يستخدم للإشارة إلى عملية يتم بواسطتها نسخ محتويات ملف منطقة نطاق

من مزوِّد خدمة أساسي إلى مزوِّد خدمة آخر ثانوي.

٧٠. صفحات المزوِّد النشطة Active Server Pages (ASP)

وهي تقنية تمكن المطورين للبرامج من إنتاج صفحات تفاعلية ديناميكية.

٧١. مشغل نصوص جافا JavaScript

لغة طورتها كل من شركتي Sun Microsystems وNetscape، لتسهيل إضافة مزايا تفاعلية إلى صفحات ويب. وعلى الرغم من كونها مشتقة من لغة جافا، إلا أنها تمثل لغة منفصلة، وإلى حد ما، أكثر سهولة، وتنحصر فاعليتها في جهة الزبون client، حيث أن المفسر interpreter، الذي ينفذ تعليماتها، يكون مدمجاً في المتصفح.

٧٢. أجاكس (اختصار لـ JavaScript و XML)

أجاكس، عبارة عن شفرة تسمح ببرمجة الموقع الإلكتروني بشكل يسمح للزوار بالحصول على المحتوى شيئاً فشيئاً خلال تصفحهم للموقع. ويسهّل أجاكس طريقة استخدام الموقع ويخفف العبء على الملقمات. ولكنه يجعل من الصعب تحقيق ربح عن طريق الدعايات، ويصعّب أيضاً من عملية قياس أنواع معينة من سلوك المستخدم بالمقارنة مع المواقع «المسطّحة».

٧٣. جافا Java

لغة برمجة كائنية object-oriented، طورتها شركة Sun Microsystems، وتستخدم لإضافة الرسوم المتحركة، وأسعار البورصة الفورية، وغيرها من المزايا الديناميكية إلى الصفحات البيتية. تتيح لغة جافا إمكانية كتابة برامج تطبيقات صغيرة applets يمكن إرسالها من المزوِّد server إلى المتصفح، الذي يستطيع فك ترميزها وتنفيذها، بواسطة ما يسمى آلة جافا الافتراضية (Java virtual machine (JVM، وهذه الآلة مدمجة أصلاً في لغة «جافا»، أو أنها تضاف إليه. وينبغي «لآلة جافا الافتراضية»، أن تكون متوافقة مع المنصة التي تعمل عليها، أما «جافا» فيمكن تنفيذها على أي منصة تحتوي على آلة «جافا الافتراضية»، سواء كانت منصات بيئة «ماكنتوش» أو «ويندوز» أو غيرهما، ولذلك توصف لغة «جافا» بأنها

مستقلة عن المنصة platform independent. وتوفر آلة جافا الافتراضية تدابير أمنية لحماية موارد وبيانات الكمبيوتر، الذي يستضيفها من احتمالات العبث والتخريب. وتوفر معظم برامج التصفح شائعة الاستخدام، الدعم للغة «جافا». وتعكف شركة صن حالياً على تطوير رقاقات معالجات خاصة لتشغيل تطبيقات «جافا» بكفاءة عالية، دون الحاجة إلى آلات «جافا الافتراضية». وتعمل العديد من الشركات على إنتاج أدوات تطوير خاصة بلغة جافا. وفيما لا تدير مايكروسوفت ظهرها للغة جافا، فإنها تنتهج سياسة مناوئة لشركة صن، فيما يتعلق بمواصفاتها، وهي تجاهد من جهة أخرى للترويج لتقنيتها المنافسة، ActiveX.

٧٤. أكتيف إكس ActiveX

اسم تطلقه «مايكروسوفت Microsoft» على مجموعة تقنياتها الكائنية object-oriented، التي تهدف إلى تحقيق إمكانية إدخال مزايا ديناميكية إلى صفحات ويب. ويفترض، من الناحية النظرية على الأقل، أن تقدم ActiveX بديلاً عن لغة «جافا» من شركة صن مايكروسيستمز Sun Microsystems. ولغة ActiveX لا تحظى حالياً؛ إلا بدعم عدد محدود من المطورين، بالإضافة إلى منتجات مايكروسوفت المرتبطة بمتصفح مكتشف الإنترنت Internet Explorer. وتعد مايكروسوفت ActiveX جزءاً أساسياً من استراتيجيتها، وتخطط في أن تستمر في دعمها وتطويرها، لتصبح أداة قياسية.

٧٥. تحميل الملفات File Upload

يعبر هذا المصطلح عن عملية إرسال المعلومات من نظام محلي أو حاسوب شخصي إلى نظام في منطقة جغرافية أخرى ليتم تخزين نسخة من المعلومات في ذلك النظام، وهو عكس مصطلح download، الذي يعني استقبال المعلومات من أحد المواقع في شبكة الإنترنت.

٧٦. زر الإرسال SUBMIT Button (or Submit key)

هو مفتاح تفاعلي يتولى إرسال المعلومات إلى وجهتها في شبكة الإنترنت عند النقر عليه بالفارة.

٧٧. هجوم نصوص الموقع المتقاطعة Cross-Site Scripting (CSS) Attack

هو هجوم بدأ استخدامه منذ أن بدأت شركتا «نتسكيب» و«جافا»، من تمكين المستخدمين لإرسال النصوص والجمل البرمجية من خلال متصفح الإنترنت. والسبب الرئيس الذي أوجد الثغرة الأمنية؛ هو قدرة المستخدم على فتح نافذتين في وقت واحد، مما يسمح للمخرب من الحصول على المعلومات الحساسة من خلال التنقل بين النافذتين. وفي محاولة لحل هذه المشكلة، بدأت المتصفحات في استخدام سياسة المصدر الواحد (Same Origin Policy). وهي استراتيجية تسمح بتبادل المعلومات بين نافذتين، ولكنها لا تسمح للمخربين بالوصول إلى المعلومات الحساسة من خلال نوافذ الجافا (JavaScript)، ونظراً لأن الرمز «CSS»، معتمداً لأكثر من مصطلح في برمجة المواقع الإلكترونية، مثل «صفحات الأسلوب المتعاقبة» (Cascading Style Sheets) و(Content-scrambling System)، فقد استعيض عنه بـ«XSS». وكان أول من استخدم هذا الاختصار هو ستيف شامبيون في مقالته عام ٢٠٠٢م.

٧٨. الاصطياد Fishing

تستخدم مجازاً لاصطياد المعلومات، أو الحصول عليها بأساليب خداعية. وهذا الاصطلاح يشمل اصطلاح «الهندسة الجماعية».

٧٩. تسمم نظام أسماء النطاقات (DNS) Domain Name System poisoning

هو إجراء متعمد يتم وضعه بهدف خبيث، وأحياناً دون قصد، بحيث ينتج عنه نقل المعلومات المتوافرة على موقع معين إلى موقع آخر مستقبل في الشبكة، ويحصل التسمم إما بسبب خطأ في تصميم البرامج أو خطأ في تهيئته، أو بواسطة فيروس خبيث يتم تضمينه في الحاسوب المستهدف. ويسمى أيضاً DNS cache poisoning.

٨٠. تزوير (أو خداع) إجراءات الإنترنت المعيارية IP spoofing

يستخدم هذا الاصطلاح للإشارة إلى نمط إنترنت مزور يحتوي على عنوان إنترنت مزور، بهدف إخفاء شخصية المرسل، أو تقمص شخصية مزوِّد خدمة آخر. بهدف الحصول

على معلومات.

٨١. طرقة الموت Ping-of-Death

عبارة عن هجوم على الحواسيب باستخدام الأمر PING، يتضمن إرسال حزمة نمط إنترنت IP، أكبر من ٦٥,٥٣٥ بايت إلى الحاسوب المستهدف، ومع أن الحزم التي تتجاوز هذا الرقم غير مشروعة؛ إلا أن القراصنة يتبادلون تطبيقات وبرامج قادرة على تجاوز الرقم المشروع، ويمكن أن تكتشف الأنظمة التشغيلية المصممة بطريقة جيدة الحزم غير المشروعة وتتعامل معها بأمان، لكن لازال بعضها يفشل في ذلك.

٨٢. نمط التحكم في رسائل الإنترنت Internet Control Message Protocol (ICMP)

هو النمط المستخدم في نقل رسائل الخطأ والتحكم، المتعلقة بنقل حزم البيانات، وفقاً لنمط الإنترنت IP. فعندما يتعذر توصيل حزمة من نمط الإنترنت إلى العنوان، الذي تقصده والمحدد في الحزمة، وذلك؛ بسبب انشغال أو عطل طارئ في المزوِّد الهدف، أو بسبب اختناقات مرورية في توصيلات الشبكة، يصدر أحد الموجهات routers في الشبكة، رسالة ICMP لإخطار المرسل بعدم وصول الحزمة ليعيد إرسالها. انظر أيضاً نمط الإنترنت IP.

٨٣. لغة سي C language

هي لغة برمجة للاستخدامات العامة، وتعد برمجة كائنية. وينظر إليها الكثيرون على أنها اللغة الأفضل لتصميم التطبيقات ذات الواجهة الكبيرة، وللتعامل مع البنية الصلبة للحاسب. وهي من لغات البرمجة العالية المستوى، وفي الوقت نفسه فإنها قريبة من لغة التجميع ذات المستوى المحدود. كما أنها تعد لغة برمجة إجرائية (يمكن بواسطتها كتابة برنامج يحتوي على إجراءات وتوابع فقط). كما أنها تعد لغة غرضية التوجه (البرنامج المكتوب عبارة عن أصناف، وتستخدم الخواص المتاحة من كبسلة وتعددية الأشكال والوراثة والتركيب).

٨٤. الترميز المصدر Source Code

الترميز المصدر، هو باختصار برنامج يقدم الرموز البرمجية الأساسية، التي يبنى بها البرامج التطبيقية، وهو يحدد كيفية عمل التطبيق وأسلوب برمجته، ويمكن لأي متخصص في لغة البرمجة المكتوب بها «الترميز المصدر» أن يطور التطبيق، أو يغيره، أو إضافة بعض المميزات عليه، ليتوافق مع احتياجاته، واستخداماته الخاصة؛ أو للتوزيع إذا سمح مالكه أو من كتبه بذلك. مع ملاحظة أن كلمة مفتوح المصدر لا تعني مجاني، ولكنها تعني الإطلاع على الترميز المصدر المستخدم، بحيث يمكن لأي مطور أخذه وتعديله أو الزيادة عليه.

٨٥. التهيئة الافتراضية Default Configurations

التهيئة الافتراضية، هي طريقة تنصيب البرامج الجديدة بأسلوب تلقائي، دون تغيير من قبل المستخدم. والمعروف أن جميع البرامج تعطي المستفيد منها خيارات، إما أن يقبل التهيئة التي وضعها المالك الأصلي للبرنامج؛ أو يختار تنصيب حسب رغبته والإمكانات المتوافرة لديه، بما في ذلك فتح أو قفل الموانئ التي لا يرغب في استخدامها وتعطيل بعض خصائص التطبيق التي لا يحتاجها.

٨٦. العيوب في تهيئة النظام System Configuration Bugs

تصل معظم الأنظمة للمستفيد النهائي بتهيئة افتراضية تسهل الاستخدام، ولسوء الحظ فإن سهولة الاستخدام تعني سهولة الاختراق. وفي السنوات الأخيرة تنبه مصممو البرامج والأنظمة لهذه المشكلة، وبدءوا في إصدار أنظمة ذات قدرات أمنية أفضل، ولكن لا زال هناك مخاطر مرتبطة بالتهيئة الافتراضية.

٨٧. تشغيل خدمات غير ضرورية Running Unnecessary Services

في معظم الأحيان يقوم مدير النظام، أو الشخص الذي ينصب البرنامج؛ بفتح ميناء أو بوابة في النظام، أو تشغيل بعض الوظائف التي لا يحتاجها، مع أن جميع تعليمات التنصيب تنص بشدة على ضرورة قفل كل وظيفة أو بوابة ليس لها حاجة ضرورية و أساسية في الجهاز أو النظام، لضمان عدم إحداث ثغرات عرضية غير متوقعة.

٨٨. عيوب التصميم Design Flaws

هي عيوب وثغرات تكون موجودة في أصل التصميم، تمكن المهاجمين من الدخول للبرنامج أو النظام، وهي منتشرة بصورة خاصة في البرامج التطبيقية وبيئات التشغيل، إذ إن كثيراً من أنماط الإنترنت مثل: نمط التحكم في الإرسال والإنترنت TCP/IP صممت قبل أن يكون هناك تجارب بالهجوم الواسع والمتسارع الذي يُلحظ اليوم في الشبكة، ونتيجة لذلك ظهرت عيوب تصميمية متعددة، تقود إلى احتمالية وجود مشاكل أمنية كثيرة.

٨٩. هجوم سميرف SMURF

هذا الهجوم، أخذ اسمه من اسم البرنامج الذي ينفذه «برنامج SMARF»، وهو عبارة عن طريقة تمكن المهاجم من إرسال كمية محدودة من الحركة المرورية الإلكترونية، التي تتسبب في إثارة تضخم في الحركة المرورية للنظام المستهدف، على هيئة انفجار تفاعلي يتضخم في الموقع الهدف، يؤدي إلى إغراقه وتعطيله. وهو يستخدم غالباً أداة «الطرق Ping»، إذ يرسل حزمة من الرموز إلى النظام ويقيس وقت انتقال الحزمة من جهاز المهاجم إلي المزوِّد المستهدف، وعودتها إلى جهازه الموجود في موقع آخر قد يكون في نفس المكان أو في بلد آخر. وكذلك تسجيل أي جزء يفقد من الحزمة.

٩٠. عناوين البث الموجه directed broadcast addresses

وهي عبارة عن إجراءات، يقوم به نمط عنوان الإنترنت IP، الذي يحدد جميع المواقع المضيفة المراد التواصل معها، في شبكة معينة. مع ملاحظة أن نمط عنوان الإنترنت يوجه نسخة واحدة من البث الموجه لكل شبكة محددة، وتتولى تلك الشبكة البث لجميع النهايات والشبكات المرتبطة بها.

٩١. لغة الاستعلامات البنيوية SQL

هي لغة برمجة تقوم بإرسال استعلامات لتجميع بيانات العديد من المواقع والتطبيقات، وهي تعمل من وراء الكواليس في المدونات وعناصر التحكم في الآلات المنقولة (Widget) وفي بعض المواقع الإلكترونية.

٩٢. برنامج ويدجت Widget

هو عبارة عن برنامج تطبيقي صغير مستقل يتم تشغيله من قبل محركات تسمى محركات ويدجت Widget Engines، وكثيراً ما تستخدم لتشغيل البرامج المتعلقة بالطقس، والمناخ، وقوائم الأسواق المالية، وبرامج تتبع قوائم رحلات الطيران، وعرض الدعايات والخرائط، كما أنها تسمح بتشغيل عدة برامج صغيرة في وقت واحد.

٩٣. المضيفات Hosts

هي المواقع التي تستضيف الصفحات البيتية، سواءً كانت هذه المواقع مجانية أو مقابل رسوم مالية.

٩٤. البوابات Portals

البوابة، عبارة عن موقع إلكتروني يقدم أنماطاً ونماذج متعددة من المحتوى. وتتشعب منه صفحات أخرى لها علاقة بالشركة أو المنظمة المالكة للبوابة، فتقدم المحتوى الخاص بها كجزء من الموقع الرئيس. بينما يحتوى الموقع على أجزاء أخرى مثل: مواقع تشمل تفاصيل عن خدمة معينة من خدماتها، ومحركات البحث الخاصة بها، والتطبيقات الرقمية والتقويمات الشخصية وغيرها.

٩٥. العنكبوت Spider

العنكبوت؛ عبارة عن برنامج تستخدمه محركات البحث للتجول في شبكة الإنترنت أثناء عملية البحث، لجمع المعلومات من مواقع الإنترنت وقواعد البيانات المتوافرة في الشبكة، ومن ثم تقوم بتبليغ محركات البحث عن هذه المعلومات (مثل المواقع المتوقفة عن العمل أو التحديثات الجديدة في الموقع وغيرها).

٩٦. تصنيف أو (وصف) الصفحة Page Description

المقصود بالتصنيف، الطريقة التي يتم فيها تقسيم المواد. والتصنيف الجيد يمكّن محركات البحث من إيجاد المحتوى على الموقع الإلكتروني وأرشفته. ويحتوى التصنيف على كلمات رئيسة، وشفرة HTML، والنص المستخدم على الموقع.

٩٧. ويكي WIKI

اصطلاح جديد يستخدم في العادة من قبل أعضاء في مجموعة معينة؛ لإنشاء وتطوير، وتحرير وتعديل صفحة بيتيه، أو كتاب بطرق تعاونية، وفي الغالب تكون هذه الصفحة مفتوحة أمام المستخدمين. ويعد موقع ويكيبيديا أفضل مثال عليه. والكلمة مأخوذة من لغة الهنود الحمر، وهي تعني مكان تجمعهم عندما يريدون مناقشة قضية تخص القبيلة.

٩٨. خلفية الموقع Site Background

عبارة عن مصطلح يطلق على كل شي يحدث خلف واجهة التصميم، ويشمل أسلوب البناء، وقواعد البيانات، والأرشيف، ونظام إدارة المحتوى، وغيرها من العناصر التي تدعم الموقع الإلكتروني.

٩٩. شريط الأدوات Tools Bar

شريط الأدوات عبارة عن قوائم تشمل بعض الأوامر، وهو في الغالب موجود في مستعرض الصفحات، ومهمته تجميع وعرض عناوين مواقع الإنترنت المختلفة والوثائق والملفات الصوتية وغيرها من المحتوى المتوافر على شبكة الإنترنت. ويمكن تخصيص أشرطة الأدوات بحسب المحتوى.

١٠٠. مدونة الفيديو Vlog

عبارة عن مدونة تم إنشاؤها لعرض أفلام الفيديو فقط مع وجود نص قصير معه، ويتم تحديثها باستمرار، ويمكن الاشتراك بها مقابل رسوم محددة، وهي تمكن من نشر تدوين الفيديو على مواقع الإنترنت أو على برنامج iTunes أو عن طريق أدوات أخرى مثل YouTube.

١٠١. الشبكة الدلالية Semantic Web

وهي تسمية جديدة للشبكة العنكبوتية العالمية. ويطلق عليها أحياناً مصطلح WEB3، ويعرِّفها آخرون بلغة الويب الطبيعية. فهي تسهّل إجراء اتصالات من غير تدخل إنساني واضح، وقد تنبأ بها أحد مخترعي الإنترنت، وهو السير تيم بيرنز لي في عام ١٩٩٩م بقوله: «لدي حلم متعلق بالويب، إذ ستصبح أجهزة الحاسوب قابلة على تحليل البيانات على الإنترنت، بما

في ذلك المحتوى، والوصلات، والتعاملات ما بين الأشخاص، وأجهزة الحاسوب. والشبكة الدلالية التي ستجعل هذا ممكناً، لم تظهر بعد، ولكن عندما يأتي هذا اليوم فسيتم التعامل مع آليات التجارة اليومية، والبيروقراطية، و حياتنا اليومية، من قبل أجهزة تتحدث مع أجهزة أخرى».

١٠٢. أسئلة يتكرر طرحها FAQ Frequently Asked Questions

وثيقة تتضمن إجابات عن أسئلة في مجال معين، يتكرر طرحها عبر الشبكة العالمية. وتتوافر وثائق FAQ في مواقع كثيرة في الإنترنت، وهي تغطي نطاقاً واسعاً ومتنوعاً من المعلومات، من فن الطبخ وحتى آليات عمل أنماط TCP/IP، وكتابة البرامج وغير ذلك.

١٠٣. حرب الكلمات Flame

هي حرب تحريرية تنشأ بين مشاركين في إحدى مجموعات النقاش، أو القوائم البريدية، بسبب طرح تعليق شخصي غير مناسب، أو محاولة بث رسائل ترويج تجارية لمنتج ما، أو غيرها من التصرفات غير اللائقة، ويعاقب الشخص المسيء، عادة، بأن يرسل له أعضاء المجموعة أو القائمة البريدية، مجموعة كبيرة من الرسائل الإلكترونية، مرفقاً بها ملفات ضخمة الحجم، لتبديد وقته أثناء تفحصه لصندوق بريده الإلكتروني، وإغراق قرصه الصلب بملفات ضخمة لا فائدة منها.

١٠٤. تكلفة عروض الصفحات (CPM) cost of page views per thousand

هي التكلفة، التي يحددها الموقع لنشر الإعلان، حسب عدد عروض الصفحات، مقدرة بالآلاف. ويرمز الحرف M في CPM، إلى «الألف» باللغة الرومانية القديمة، وليس إلى مليون أوميجا. ويستخدم مندوبو المبيعات، أحياناً، مصطلح CPM للدلالة على تكلفة عروض الإعلانات، لأنه من الصعب ضمان أن يؤدي عرض الصفحة دوماً، إلى عرض الإعلان، فقد يختفي الإعلان من الصفحة بسبب الزائر.

١٠٥. نقرة Click

هو النقر على الأيقونة للذهاب للتشعيب المخصص لها، وعلى سبيل المثال؛ عندما ينقر المتصفح فوق إعلان موجود على الصفحة، فإنه ينتقل من خلال الوصلة التشعيبية إلى موقع الشركة صاحبة الإعلان.

١٠٦. تيار النقرات Click Stream

هو المسار، الذي يسلكه المستخدم خلال تصفحه الموقع. وتساعد معلومات تيار النقرات مدير الموقع على معرفة كيفية استخدام الزوار للموقع، وأي الصفحات تنال الاهتمام الأكبر، كما تساعد المعلن، أيضاً، على تحديد موقع الصفحات المناسبة، لوضع إعلاناته ضمنها.

١٠٧. نقرات العبور Click Through

يستخدم هذا المصطلح بالتبادل مع «نقرة»، للدلالة على عدد المرات التي عبر منها الزائر إلى الموقع المعلن، بالنقر على أيقونة معينة في صفحة ويب الخاصة بالشركة المضيفة. ويفضل المعلنون أن يدفعوا ثمناً لنقرات العبور، بدلاً من عروض الإعلان، لأن الزائر قد يرى الإعلان، لكن بدون أن ينقر فوقه للذهاب إلى موقع المعلن.

١٠٨. حزمة Packet

هي جزئية من البيانات، تنشأ نتيجة لتقسيم الرسالة المتضمِنة للمعلومات المراد نقلها عبر الشبكة، إلى كتل صغيرة، تضاف إليها بيانات خاصة بالتحكم في النقل وعنوان الوجهة التي تقصدها. وترسل هذه الحزم فرادى، عبر المسارات المتاحة في الشبكة، ويعاد تجميعها عندما تبلغ وجهتها فتعود لهيئتها الأصلية، وتستخدم تقنية تجزئة البيانات إلى حزم في الغالبية العظمى في الشبكات الرقمية فائقة السرعة، وهي تمثل أساس مجموعة أنماط TCP/IP، المستخدمة في إنترنت.

١٠٩. قوائم البريد Mailing List

تشير العبارة بشكل عام إلى قوائم تضم عناوين للبريد الإلكتروني، تُشكل آلياً، أو

يدوياً. لغرض استخدامها في توجيه رسائل إلكترونية إلى الجهات، التي تتضمنها هذه القوائم، ويمكن للغالبية العظمى من برامج البريد الإلكتروني، تكرار بث رسالة معينة، إلى قائمة تضم مجموعة من العناوين. وهي تشير إلى مجموعة من المستخدمين الذين ينتسبون إلى جهة معينة، بهدف تلقي الرسائل التي تصدرها حول موضوع محدد، وتصل مثل هذه الرسائل تلقائياً، إلى جميع المسجلين في القائمة. وازدهرت قوائم البريد في الماضي، عندما كانت بالنسبة للكثيرين الوسيلة الوحيدة للحصول على معلومات عبر الشبكة، إلا أن الكثير من هذه القوائم الكبيرة استبدلت، فيما بعد، بالمجموعات الإخبارية newsgroups. وتستخدم قوائم البريد حالياً، لنشر المعلومات عن موضوعات شديدة التخصص، ولنشر الرسائل في المجموعات المغلقة، ولأغراض الترويج التجاري، حيث يتطفل مرسلوها، بصرف النظر عن رغبة المتلقي.

١١٠. التفاوض التلقائي Auto-Negotiation

الاسم الرسمي له National Semiconductor`s N-Way، وهي تقنية تسمح بتحديد سرعة الوصلة، واتجاه الإرسال آحادي أم ثنائي، بين أجهزة إيثرنت، حسب إمكانياتها.

١١١. العمود الفقري (للشبكة) Backbone

يقصد بالعمود الفقري Backbone في سياق الحديث عن الإنترنت، بأنه مجموعة الوصلات السريعة، التي تصل بين الحواسيب المضيفة حول العالم في إطار شبكة الإنترنت. وكلما كانت الصلة بين الحاسوب والعمود الفقري مباشره ودون وسيط، أو من خلال وصلات قليلة، أو عن طريق وصلات سريعة يكون الاتصال بالإنترنت أفضل من الناحية النظرية.

١١٢. التشفير Encryption

هي عملية تحويل البيانات، التي على شكل نصوص واضحة وميسرة plaintext، إلى هيئة يصعب قراءتها وفهمها دون عملية معاكسة تسمى إزالة التشفير decryption، تعيدها إلى هيئتها الأصلية. وفيما لا توجد طريقة في التشفير من شأنها توفير الحماية المطلقة للبيانات على المدى البعيد، فإن الأبحاث الحديثة توصلت إلى أساليب في التشفير، تجعل من المستحيل

إعادة النصوص المشفرة إلى هيئتها الأصلية دون امتلاك «مفتاح التشفير «encryption key»». ويتفق خبراء الإنترنت على أهمية تحقيق تشفير محكم للمعلومات الخاصة ببطاقات الائتمان التي ترسل عبر الشبكة في سياق عمليات التجارة الإلكترونية، كشرط لتشجيع الناس على الإقبال على التعامل مع هذا النوع من التجارة.

١١٣. **الكيك** Cookie

تشير هذه العبارة؛ إلى ملف أو سجل بيانات، يُسجل على القرص الصلب للحاسوب بواسطة حاسوب آخر متصل معه من خلال الشبكة وفي الغالب دون معرفة مالك الحاسوب، وتتيح البيانات المدونة في الملف cookies، للمزوِّد server الذي وضعه، معرفة المواقع التي تمت زيارتها في الآونة الأخيرة، ومعلومات أخرى يريدها واضع الملف، و القليل من المزوِّدات في الإنترنت، تستأذن في تسجيل الملف أو قراءة معلومات في الملف cookies، ويعدها كثيرون انتهاكاً لحرمة خصوصياتهم. وظهرت العديد من البرمجيات المضادة anti-cookie، التي تبادر إلى محو أية بيانات تسجل في الملف cookies فور حدوثها.

١١٤. **توقيع رقمي** Digital Signature

عبارة عن بيانات تضاف إلى الرسائل الإلكترونية، لإثبات هوية مرسلها، وسلامة محتوياتها خلال التبادل، ويستخدم المرسل دالة خاصة (hash function) لتوليد رقم معين، يسمى التوقيع، بالاعتماد على محتويات الرسالة، ثم يشفر التوقيع الناتج ويضيفه إلى الرسالة، باستخدام مفتاح تشفير خاص، ويعيد المتلقي الرقم الناتج بتطبيق الدالة ذاتها على نص الرسالة (دون الرقم المشفّر). ويفك تشفير التوقيع باستخدام مفتاح التشفير العمومي الخاص بالمرسل (الذي يعرفه المتلقي مسبقاً)، ويقارن بين الرقمين. ويدل تطابق الرقمين على أن محتويات الرسالة وصلت سليمة دون أي تشويه، وأنها تحمل توقيع المرسل الصحيح.

١١٥. **سُلْطة التصديق** Certificate of Authentication (CA)

هيئة معتمدة، يتم الرجوع إليها للتحقق من هوية أفراد أو شركات معينة ناشطة على الإنترنت، أو هوية ومصدر عناصر، مثل ActiveX، والحصول على شهادات رقمية تثبت أن الفرد أو الشركة أو العنصر معروف من قبل هذه السلطة، ولا ضير في التعامل الإلكتروني

معها. وقد نشأت سلطات التصديق لتلبية متطلبات التجارة الإلكترونية، لضمان حقوق المتعاملين بها عبر الإنترنت بشكل رئيسي، ويمكن أن تكون سلطة التصديق شركة مستقلة، مثل VeriSign، وعندها تعد مرجعاً عاماً، أو تكون قسماً داخلياً في شركة، مثل قسم الحاسوب، فتكون شهاداتها معتمدة ضمن الشركة ذاتها، أو مع بعض الشركات التي تتعامل معها.

١١٦. مواطن الشبكة Netizen

مصطلح مختصر للعبارة Internet citizen، التي تعني «مواطن الشبكة»، ويشير هذا المصطلح إلى حالة الأفراد الذي يشعرون بانتماء قوي إلى شبكة إنترنت معينة، وكأنها موطنهم، فيراعوا قوانينها المكتوبة وغير المكتوبة، ويحرصوا على سلامتها وأمنها، ويهتمون بتطورها ومستقبلها. ويوصف مثل هؤلاء بأنهم مواطنو شبكة صالحون «Good Citizen».

١١٧. النقد الإلكتروني CyberCash

هو أحد الأنظمة لدفع النقود، بواسطة الشيكات الإلكترونية أو بطاقات الائتمان، طورته شركة CyberCash Inc، وتستخدمه مزوِّدات التجارة الإلكترونية، لتدقيق معلومات بطاقات الائتمان، ومعالجة المدفوعات، لقاء رسوم يسيرة تدفعها للشركة. ويلجأ الأفراد إلى نظام CyberCash للحصول على شيكات إلكترونية، لاستخدامها في عمليات الشراء عبر إنترنت، لقاء بعض الرسوم، أيضاً.

١١٨. كويك تايم QuickTime QT

وهي معمارية خاصة ابتكرتها شركة أبل، للتعامل مع البيانات الحساسة لعنصر الوقت، مثل الصوت والفيديو. وهي تمتاز بالقدرة على التوفيق ما بين عدد من مسارات الصوت والصورة، وكذلك ضغط البيانات، وإزالة الضغط عنها (compression decompression)، لإعادتها إلى هيئتها الأصلية، واعتماد هيئة عامة للبيانات، يمكن التعامل معها بواسطة نظم غير متوافقة. وتتوفر وظائف QuickTime كتوسعة لنظام تشغيل ماكنتوش، في حين أنها تعتمد في نظم الحواسيب الشخصية على برنامج مكتبة الربط الديناميكي DLL، وهو هيئة ملف بيانات يتوافق مع مواصفات QuickTime.

حروب تقنية المعلومات

كيف يشنها القراصنة والإرهابيون على البنية التحتية العالمية؟ وكيفية مواجهتها؟

الكتاب الذي بين يدي القارئ حصيلة خبرة أكثر من خمسة وعشرين عاماً متواصلة في مجالات الأمن بصورة عامة وأمن المعلومات على وجه الخصوص، تم التعامل معها عن قرب، وكان من الواجب الأخلاقي والوطني وضعها بين يدي القارئ الكريم، مدعومة بما تجمَّع خلال هذه الفترة الطويلة من معلومات تقنية واستخباراتية تتعلق بمكافحة الإرهاب وحماية شبكات الاتصالات بصورة عامة وشبكات الاتصالات الحكومية على وجه الخصوص، بأسلوب ميسر بعيد عن التعقيدات الفنية لتعم الفائدة. ويتكون الكتاب من ثلاثة أبواب: الباب الأول يتألف من ثلاثة فصول، الفصل الأول عبارة عن تمهيد تم الحديث فيه عن تعريف البنية التحتية للإرهاب وتوضيح اعتمادها بشكل كامل على تقنية صناعة المعلومات. كما تناول الفصل الأول بدايات الإنترنت وتطورها حتى وصلت إلى ما وصلت إليه. وفي الفصل الثاني كان من الضروري تقديم نبذة للقارئ الحريص على معرفة تقنيات اختراق الحواسيب وسرقة أو معرفة ما يخزن فيها من معلومات كتبت بأسلوب مبسط ليفهمها غير المتخصصين. وطرح في الفصل الثالث بنوع من الإسهاب استخدامات القراصنة والإرهابيين لكافة الوسائل التقنية بما فيها الوسائط المتعددة والإعلام الجماعي، والحديث عن بعض مواقع قراصنة المعلومات وإرهابيي الإنترنت واستخداماتهم لتقنية المعلومات المفتوحة والبرمجيات والأدوات المجانية المفتوحة المصدر.

وقسِّم الباب الثاني من الكتاب إلى ثلاثة فصول، تم تخصيصها للتهديدات التي تقع على البنية التحتية منذ فجر التاريخ، وحتى هذه الأيام. وتصنيف فشل وإخفاقات الأنظمة وكيف يفكر القراصنة والإرهابيون؟ ولماذا يمتهنون هذه المهنة غير الأخلاقية؟ وطريقة اختيارهم للثغرات الأمنية، وطرحت أمثلة للعمليات الإرهابية والكوارث الطبيعية وتأثيراتها في الاقتصاد الدولي وتصنيف مفصلٌ لما يعتبر إخفاقات وأسباب هذه الإخفاقات وتحديد المخاطر التي تعترض البنية التحتية. أما الباب الثالث والأخير من الكتاب فقد خصص للحلول والإجراءات الواجب اتباعها لحماية البنية التحتية بكافة عناصرها ومكوناتها.

فريج بن سعيد العويضي

